Commissaire du Centre de la sécurité des télécommunications

RAPPORT ANNUEL 2017–2018

Canada

Bureau du commissaire du
Centre de la sécurité des télécommunications
C.P. 1474, succursale « B »
Ottawa (Ontario) K1P 5P6

Téléphone : 613-992-3044
Télécopieur : 613-992-4096
Site Web : www.ocsec-bccst.gc.ca

© Sa Majesté la Reine du Chef du Canada, représentée par le
Bureau du commissaire du Centre de la sécurité des télécommunications, 2018

N° de catalogue : D95F-PDF
ISSN 1700-0882

Commissaire du Centre de la
sécurité des télécommunications

L'honorable Jean-Pierre Plouffe, CD

Communications Security
Establishment Commissioner

The Honourable Jean-Pierre Plouffe, CD

Juin 2018

Ministre de la Défense nationale
Édifice MGén George R. Pearkes, 13e étage
101, promenade Colonel By, tour Nord
Ottawa (Ontario) K1A 0K2

Monsieur le Ministre,

Conformément au paragraphe 273.63(3) de la *Loi sur la défense nationale*, j'ai l'honneur de vous transmettre le rapport annuel faisant état de mes activités et constatations pour la période allant du 1er avril 2017 au 31 mars 2018, aux fins de présentation au Parlement.

Je vous prie d'agréer, Monsieur le Ministre, l'assurance de ma haute considération.

Jean-Pierre Plouffe

C.P. / P.O. Box 1474, succursale « B » / Station "B"
Ottawa ON Canada K1P 5P6

TABLE DES MATIÈRES

Message du commissaire 3

Le mandat et les activités d'examen du commissaire 6

Le point sur les efforts déployés par le CST pour donner suite aux recommandations 9

Aperçu des constatations et des recommandations de 2017–2018 12

Points saillants des rapports présentés au ministre en 2017–2018 14

1. Examen des pouvoirs du CST et de sa participation à une initiative opérationnelle multilatérale 14
2. Étude sur l'utilisation opérationnelle par le CST de plateformes internes de type média social 19
3. Examen annuel des divulgations d'information sur l'identité de Canadiens par le CST, 2015–2016 23
4. Examen annuel des divulgations d'information sur l'identité de Canadiens par le CST, 2016–2017 28
5. Examen annuel des activités de cyberdéfense du CST menées sous le régime d'une autorisation ministérielle, 2016–2017 31
6. Examen combiné annuel des autorisations ministérielles du CST relatives à la collecte de renseignements électromagnétiques étrangers, 2016–2017 et 2017–2018 et vérification ponctuelle des « communications canadiennes » 38
7. Examen annuel des Dossiers relatifs aux incidents liés à la vie privée et du Dossier des erreurs de procédure mineures 46

Plaintes concernant les activités du CST 50

Mandat sous le régime de la *Loi sur la protection de l'information* 50

Activités du bureau du commissaire 50

Plan de travail – Examens en cours et prévus 55

Annexe A : Biographie de l'honorable Jean-Pierre Plouffe, CD 56

Annexe B : Extraits de la *Loi sur la défense nationale* et de la *Loi sur la protection de l'information* relatifs au mandat du commissaire 57

MESSAGE DU COMMISSAIRE

Alors que mon deuxième mandat touche à sa fin, je fais le bilan d'une année bien remplie et satisfaisante. J'ai le privilège d'être le commissaire du Centre de la sécurité des télécommunications en cette période cruciale où le gouvernement s'emploie à réviser le cadre de reddition de comptes en matière de sécurité nationale.

Premièrement, le projet de loi C-22 a constitué le Comité des parlementaires sur la sécurité nationale et le renseignement. Au moment où ce projet de loi a reçu la sanction royale en juin 2017, le projet de loi C-59 a été déposé, prévoyant l'octroi de nouveaux pouvoirs aux organismes de sécurité et de renseignement afin de leur permettre de contrer une menace en évolution ainsi que de protéger le Canada et les Canadiens tout en élargissant la surveillance de façon générale. Nous tous qui œuvrons dans le domaine de l'examen et sommes touchés par cette loi et ce projet de loi devons nous efforcer de veiller à ce que ceux-ci renforcent véritablement la reddition de comptes des organismes de sécurité et de renseignement du Canada. Une dimension inhérente à cette reddition de comptes consistera à s'assurer que nous continuons également à faire preuve de la plus grande transparence possible, afin que le public comprenne mieux de quelle façon ces organismes sont tenus de rendre des comptes, alors qu'ils doivent en grande partie mener leurs activités en secret, de même que le degré de rigueur qui est exercé à cet égard. De par leur étendue, les changements en cours peuvent sembler intimidants toutefois, l'adoption d'une démarche stable et concertée pendant la période initiale nous aidera à atteindre les objectifs visés, qui seront ultimement déterminés par le Parlement.

Le projet de loi C-59 est complexe et d'une très grande portée. Il propose d'apporter aux lois, aux activités et aux mécanismes de reddition de comptes en matière de sécurité nationale les modifications les plus importantes depuis que la ***Loi sur le Service canadien du renseignement de sécurité*** a été adoptée il y a presque trente-cinq ans, dans le but de créer le Comité de surveillance des activités de renseignement de sécurité et le poste d'inspecteur général. Le projet de loi C-59 vise à établir trois nouvelles lois et à modifier cinq lois existantes. Mon rôle actuel consistant à examiner les activités antérieures du Centre de la sécurité des télécommunications (CST) sera assumé exclusivement par un nouvel organisme d'examen, soit l'Office de surveillance des activités en matière de sécurité nationale et de renseignement, lequel sera chargé d'examiner toute activité liée à la sécurité nationale menée par tout ministère ou organisme gouvernemental. Ce projet de loi prévoit la création d'une autre loi, à savoir la ***Loi sur le commissaire***

au renseignement, en vertu de laquelle mon bureau effectuera la transition vers un nouveau rôle quasi judiciaire. Je participerai au processus décisionnel en examinant les autorisations ministérielles concernant certaines activités du CST et du Service canadien du renseignement de sécurité (SCRS). Si je suis convaincu, au terme de mon examen, que les autorisations signées par le ministre sont raisonnables, j'aurai le pouvoir, à titre de commissaire au renseignement, de les approuver. Ce n'est qu'ensuite que les activités visées pourront être exécutées.

Je surveille avec grand intérêt le cheminement du projet de loi au Parlement. Dans la mesure du possible, je veux m'assurer que le projet de loi ne recrée pas les problèmes qui ont hanté la partie V.1 de la *Loi sur la défense nationale*. Adoptée en 2001, la partie V.1 comportait des ambiguïtés qui, malgré les recommandations formulées à maintes reprises par mes prédécesseurs et moi-même, n'avaient jamais été traitées avant aujourd'hui, c'est-à-dire dans le cadre du projet de loi C-59. Cependant, ce projet de loi renferme des ambiguïtés en soi. À cet effet, j'ai présenté plusieurs observations au Comité permanent de la sécurité publique et nationale (SECU) de la Chambre des communes qui se penchait sur le projet de loi C-59. J'ai présenté des propositions de modifications visant à assurer la clarté et à éviter l'ambiguïté. Les autres modifications que j'ai proposées permettraient, à mon avis, d'ajouter un certain niveau de souplesse dans le but d'accroître l'efficience du processus d'examen et d'approbation, par le commissaire au renseignement, de certaines autorisations ministérielles pour le CST et le SCRS.

Le Canada n'est pas le seul pays à apporter des changements importants à ses pouvoirs et à ses mécanismes de reddition de comptes en matière de sécurité nationale. D'autres pays ont aussi répondu à la demande de nouveaux outils pour lutter contre les menaces en constante évolution tout en renforçant la reddition de comptes. Le solide partenariat entre les organismes de renseignement au Canada, aux États-Unis, au Royaume-Uni, en Australie et en Nouvelle-Zélande (la Collectivité des cinq) a ouvert la voie à une tribune permettant aux représentants des organismes d'examen et de surveillance de ces pays d'étudier des questions et des préoccupations communes ainsi que d'échanger des pratiques exemplaires. À la fin de 2016, mon collègue, le président du Comité de surveillance des activités de renseignement de sécurité, et moi-même avons convenu, avec nos homologues de ces pays, de mettre sur pied le Five Eyes Intelligence Oversight and Review Council (conseil de surveillance et d'examen des activités de renseignement de la Collectivité des cinq). Le Canada a accueilli la première réunion en personne du conseil, laquelle s'est tenue dans mes bureaux en octobre 2017. Le commissaire au renseignement continuerait de participer aux activités de ce conseil.

Le conseil ne représente qu'une partie – mais une partie importante tout de même – des efforts visant à améliorer les échanges avec les organismes d'examen et de surveillance d'autres pays. Les discussions de ce conseil peuvent contribuer

à l'efficacité du travail important que les organismes de renseignement accomplissent tout en veillant à ce que ce travail soit effectué dans les limites des autorisations légales, y compris dans le respect des droits à la vie privée dans nos pays respectifs.

Avant de conclure, je tiens à féliciter M^me^ Greta Bossenmaier pour sa nomination à titre de conseillère à la sécurité nationale et au renseignement auprès du premier ministre. Je suis reconnaissant du professionnalisme, de la franchise et de la collaboration dont elle a fait preuve dans le cadre de notre relation de travail alors qu'elle agissait comme chef du CST.

Enfin, la dernière année a été mouvementée, et j'aimerais terminer en félicitant les membres de mon personnel pour les efforts extraordinaires et soutenus qu'ils ont déployés en évaluant le projet de loi C-59 et en veillant à ce que notre contribution soit et demeure positive et constructive. Ils ont en outre amorcé avec diligence les préparatifs en vue de la transition vers un nouveau rôle de surveillance unique au Canada et anticipé les répercussions de cette transition sur les services internes de mon bureau et les nombreuses responsabilités supplémentaires qui en découlent. Enfin, ils ont garanti un dialogue constructif avec le CST et le SCRS relativement au nouveau rôle proposé du commissaire au renseignement tout en assumant les responsabilités courantes qui consistent à examiner les activités du CST pour vérifier qu'elles sont conformes à la loi et qu'elles protègent la vie privée des Canadiens, jusqu'à ce que le projet de loi C-59 soit adopté.

LE MANDAT ET LES ACTIVITÉS D'EXAMEN DU COMMISSAIRE

Le Bureau du commissaire du Centre de la sécurité des télécommunications (CST) est un organisme d'examen indépendant.

MANDAT

Le mandat du commissaire du CST est énoncé à la partie V.1 de la ***Loi sur la défense nationale*** :

1. procéder à des examens concernant les activités du CST – y compris les activités liées aux renseignements électromagnétiques étrangers et à la sécurité des technologies de l'information à l'appui du gouvernement du Canada – pour en contrôler la légalité;
2. faire les enquêtes que le commissaire estime nécessaires à la suite d'une plainte écrite; et
3. informer le ministre de la Défense nationale (qui est responsable du CST devant le Parlement) et le procureur général du Canada de toute activité du CST qui, à son avis, pourrait ne pas être conforme à la loi.

En vertu de l'article 15 de la ***Loi sur la protection de l'information***, le commissaire a également pour mandat de recevoir de l'information émanant de personnes astreintes au secret à perpétuité qui souhaitent communiquer des renseignements opérationnels spéciaux du CST en faisant valoir la primauté de l'intérêt public.

La ***Loi sur la défense nationale*** exige que le commissaire du CST soit un juge surnuméraire ou un juge à la retraite d'une cour supérieure. Elle confère au commissaire une autonomie complète et un accès sans entrave à tous les systèmes et installations du CST, ainsi qu'à son personnel, notamment le pouvoir d'assigner à comparaître pour obliger des particuliers à répondre à des questions. Le commissaire a un budget distinct accordé par le Parlement.

CONSIDÉRATIONS EN MATIÈRE D'EXAMEN

L'approche du commissaire à l'égard des examens est à la fois basée sur les objectifs recherchés – s'appuyant sur son mandat – et préventive. Les activités du CST incluent la collecte de renseignements électromagnétiques étrangers sur des cibles étrangères se trouvant à l'extérieur du Canada, c'est-à-dire de l'information sur les moyens, les intentions ou les activités de cibles étrangères portant sur les affaires internationales, la défense ou la sécurité. Le CST est également l'organisme technique principal du Canada responsable de la cyberdéfense et de la cryptographie, ainsi que d'autres technologies qui sont requises pour protéger les

systèmes et les réseaux informatiques du gouvernement qui renferment des informations nationales et personnelles sensibles. Le CST a en outre pour mandat de mettre à profit ses capacités uniques afin de fournir une assistance technique et opérationnelle aux organismes fédéraux chargés de l'application de la loi et de la sécurité dans l'exercice des fonctions que la loi leur confère.

Les activités du CST sont distinctes des activités de collecte de renseignements criminels et en matière de sécurité menées par d'autres organismes. Il s'agit dans leur cas d'information sur des activités qui pourraient menacer la sécurité du Canada ou la sécurité publique et que l'on obtient généralement en ciblant des Canadiens en vertu de différents pouvoirs légaux. Il est expressément interdit pour ce qui est des activités du CST de viser des Canadiens ou des personnes se trouvant au Canada. Restreindre la collecte de renseignements à des cibles étrangères à l'extérieur du Canada est compliqué par l'infrastructure de l'information mondiale, qui est interconnectée et en constante évolution, ainsi que par les cibles étrangères, qui sont elles-mêmes astucieuses sur le plan technologique. Le CST a besoin de moyens techniques perfectionnés pour obtenir et analyser l'information et détecter et atténuer les cyberactivités malveillantes. Pour rester efficaces, les méthodes du CST doivent demeurer secrètes.

Dans ce contexte difficile, les agents voués à l'examen doivent posséder des connaissances spécialisées et une expertise pour comprendre les nombreux aspects techniques, juridiques et relatifs à la protection de la vie privée des activités du CST. Ils doivent également posséder des habilitations de sécurité au niveau requis pour examiner les dossiers et les systèmes du CST. Les agents voués à l'examen sont liés par la ***Loi sur la protection de l'information*** et ne peuvent pas divulguer à des personnes non autorisées les renseignements sensibles auxquels ils ont accès.

Une fois une activité sélectionnée pour examen, elle est examinée en fonction de la série de critères standards décrits ci-après :

- **Obligations légales :** le commissaire s'attend à ce que le CST mène ses activités en conformité avec la ***Charte canadienne des droits et libertés***, la ***Loi sur la défense nationale***, la ***Loi sur la protection des renseignements personnels***, le ***Code criminel*** et toute autre législation pertinente.
- **Exigences ministérielles :** le commissaire s'attend à ce que le CST mène ses activités en conformité avec les instructions ministérielles, conformément à toutes les exigences et dans le respect des limites précisées dans une autorisation ou une directive ministérielle.
- **Politiques et procédures :** le commissaire s'attend à ce que le CST dispose de politiques et de procédures pertinentes pour orienter ses activités et donner des instructions suffisantes sur les obligations légales et les exigences ministérielles, notamment en ce qui concerne la protection de la vie privée des Canadiens. Il s'attend à ce que les employés du CST soient au courant des politiques et procédures, et à ce qu'ils s'y conforment. Il s'attend aussi à ce que

le CST dispose d'un cadre efficace de validation de la conformité pour assurer le maintien de l'intégrité de ses activités opérationnelles, y compris une reddition de comptes adéquate sur les décisions importantes prises et l'information se rapportant à la conformité et à la protection de la vie privée des Canadiens.

RAPPORTS SUR LES CONSTATATIONS

Rapport classifié au ministre sur chaque examen : Les résultats des examens individuels font l'objet de rapports classifiés au ministre de la Défense nationale. Ces rapports documentent les activités du CST, renferment les constatations relatives aux critères standards et dévoilent la nature et l'importance de tout écart par rapport aux critères. Au besoin, le commissaire formule à l'intention du ministre des recommandations visant à améliorer les mesures de protection de la vie privée ou à corriger les problèmes se rapportant aux activités opérationnelles du CST mis au jour au cours de l'examen. Conformément à la pratique courante de divulgation adoptée par les vérificateurs, le CST reçoit les ébauches des rapports d'examen pour confirmation de l'exactitude des faits. Les constatations et les conclusions sont libres de toute ingérence de la part du CST ou de tout ministre.

Rapport annuel public au Parlement : Le rapport annuel du commissaire est un document public présenté au ministre qui, en vertu de la loi, doit le déposer au Parlement. Le bureau du commissaire publie les titres de tous les rapports d'examen présentés au ministre – 114 à ce jour – sur son site Web.

RESSOURCES DU BUREAU DU COMMISSAIRE

En 2017–2018, le commissaire a été épaulé par 11 employés travaillant à temps plein, eux-mêmes aidés au besoin par des spécialistes en la matière. Les dépenses du bureau se sont élevées à 1 967 061 $, montant qui se situe dans la limite du financement approuvé par le Parlement. Pour en apprendre davantage sur les dépenses du bureau, veuillez consulter son site Web.

LE POINT SUR LES EFFORTS DÉPLOYÉS PAR LE CST POUR DONNER SUITE AUX RECOMMANDATIONS

Le CST a accepté et mis en œuvre, ou travaille à la mise en œuvre, de 95 pour cent (161) des 170 recommandations formulées depuis 1997. Cela comprend les quatre recommandations que renferment les rapports de cette année. Les commissaires surveillent la façon dont le CST donne suite aux recommandations, aux constatations négatives et aux questions nécessitant un suivi relevées dans les examens. Le commissaire surveille ainsi les neuf recommandations que le CST traite actuellement, à savoir six recommandations découlant d'examens antérieurs et trois recommandations découlant de l'examen de cette année.

Au cours de la dernière année, le CST a avisé le bureau que des travaux étaient achevés en lien avec 11 recommandations antérieures. Le CST a déjà donné suite à une des recommandations de cette année.

Dans le rapport annuel du commissaire de 2008–2009, le commissaire Gonthier avait fait état de son examen des activités du CST réalisées dans le cadre d'instructions ministérielles à l'appui du mandat de collecte de renseignements électromagnétiques étrangers. Au cours de l'examen, il avait recommandé au CST d'éliminer certains écarts entre les attentes ministérielles et ses pratiques. Il avait également recommandé au CST d'examiner, de mettre à jour et d'achever les documents de politique clés portant sur ces activités et de clarifier certains termes employés dans les documents. Le CST a approuvé une version à jour de la politique opérationnelle pertinente en mai 2017 en vue de clarifier les lignes directrices relatives au programme.

Au cours de l'examen de l'autorisation ministérielle de cyberdéfense de 2015–2016, le commissaire avait recommandé au CST de diffuser des lignes directrices sur le marquage et le dénombrement uniformes de ce qui constitue des communications privées de cyberdéfense. Le CST a mis en œuvre de nouvelles directives et une formation, et a modernisé la base de données dans le but d'automatiser l'identification d'éventuelles communications privées et de normaliser le dénombrement des communications privées de cyberdéfense.

Le CST a également pris des mesures pour donner suite à la recommandation du commissaire découlant de l'examen d'une méthode particulière de collecte de renseignements électromagnétiques étrangers du CST menée sous le régime d'une autorisation ministérielle (un résumé à cet égard se trouve dans le rapport annuel de 2015–2016). Le commissaire a recommandé au CST d'éliminer les incohérences entre ses pratiques et les exigences administratives précisées dans les instructions ministérielles. En septembre 2017, le CST a mis en place un cadre de risque opérationnel en matière de renseignements électromagnétiques

étrangers. Ce cadre établit un processus d'évaluation du risque qui tient compte des risques juridiques et opérationnels ainsi que des risques liés à la réputation et aux partenariats associés aux opérations de collecte de renseignements électromagnétiques étrangers. Le programme de collecte est maintenant assorti de procédures exhaustives accessibles à tous les employés pouvant être appelés à participer à des activités dans le cadre du programme.

Au terme de l'examen du partage de renseignements du CST avec des entités étrangères de l'an dernier, le commissaire avait formulé trois recommandations. Le CST a donné suite à deux d'entre elles en juillet 2017. En ce qui a trait à la recommandation concernant l'application uniforme de mises en garde à tous les échanges de renseignements entre le CST et des entités étrangères et l'utilisation par le CST de systèmes adéquats pour consigner tous les renseignements communiqués, le CST a uniformisé le processus d'échange de renseignements avec des entités étrangères. En vue de donner suite à la recommandation selon laquelle le CST devrait diffuser des politiques stratégiques générales en ce qui a trait au partage de renseignements avec des entités étrangères, le CST a diffusé des lignes directrices qui comprennent le cadre de risque opérationnel en matière de renseignements électromagnétiques étrangers ainsi qu'une nouvelle politique.

Au cours de l'examen de l'année dernière des activités de collecte de renseignements électromagnétiques étrangers menées par le CST sous le régime d'une autorisation ministérielle, le commissaire avait recommandé que les rapports du CST adressés au ministre sur les communications privées renferment de l'information supplémentaire pour décrire plus précisément les communications privées et pour expliquer l'ampleur de l'atteinte à la vie privée. Certaines technologies de communication donnaient une vision déformée du nombre de Canadiens ou de personnes au Canada qui sont interlocuteurs dans une communication interceptée par le CST. Cette année, pour la première fois, le CST a fourni des renseignements supplémentaires au ministre pour expliquer la raison de la hausse considérable du nombre de communications privées identifiées.

Une autre recommandation provenant du rapport annuel de 2016–2017 du commissaire à laquelle le CST a donné suite portait sur les communications interceptées protégées par le secret professionnel de l'avocat. Le CST a modifié sa politique pour décrire ce que les employés du CST doivent faire lorsqu'ils traitent des communications entre un conseiller juridique et son client qui ont été recueillies dans le cadre du mandat du CST en matière de collecte de renseignements électromagnétiques étrangers.

Le CST a également donné suite à une recommandation formulée cette année au cours de l'examen par le bureau des divulgations par le CST d'information sur l'identité de Canadiens pour 2015–2016. Au terme de cet examen, le commissaire avait recommandé que le CST prenne des mesures pour veiller à ce que toutes les demandes de divulgation d'information sur l'identité de Canadiens supprimée

précisent le pouvoir légal en vertu duquel l'information est demandée et comportent une justification opérationnelle solide de la nécessité d'obtenir cette information qui est conforme au mandat de l'organisation présentant la demande. Le CST a modifié ses processus pour s'assurer que le pouvoir légal de l'organisation qui demande l'information est explicite et que la justification opérationnelle de l'organisation est solide et claire avant que le CST détermine s'il divulguera ou non l'information sur l'identité de Canadiens.

Enfin, le commissaire avait recommandé, dans le cadre de deux examens antérieurs, que des modifications soient apportées à la ***Loi sur la défense nationale***. Au cours de l'examen des activités du CST en matière de sécurité des technologies de l'information qui sont réalisées sous le régime d'une autorisation ministérielle (un compte rendu à cet égard se trouve dans le rapport annuel du commissaire de 2014–2015), le commissaire avait recommandé que le paragraphe 273.65(3) de la ***Loi sur la défense nationale*** soit modifié afin d'éliminer toute ambiguïté concernant le pouvoir du CST d'exercer des activités en matière de sécurité des technologies de l'information pouvant entraîner l'interception de communications privées. De plus, en raison d'un examen des activités du CST relatives aux métadonnées liées aux renseignements électromagnétiques étrangers à l'issue duquel le commissaire avait jugé que le CST n'avait pas minimisé de l'information sur l'identité de Canadiens avant de la partager avec des alliés, le commissaire avait recommandé que la ***Loi sur la défense nationale*** soit modifiée afin de donner un pouvoir exprès et un cadre clair en ce qui concerne les activités du CST relatives aux métadonnées. Le 20 juin 2017, le gouvernement a déposé le projet de loi C-59, ***Loi concernant des questions de sécurité nationale***. La partie 3 de ce projet de loi édicte la ***Loi sur le Centre de la sécurité des télécommunications***, qui renferme des dispositions clarifiées concernant les pouvoirs en matière de sécurité des technologies de l'information ainsi que des dispositions sur les pouvoirs de collecte et d'utilisation des métadonnées.

Le bureau est aux prises avec des questions d'interprétation juridique depuis 2001, lorsque le CST avait d'abord été établi en vertu d'une loi après les attaques terroristes survenues aux États-Unis. Depuis ce temps, les commissaires antérieurs et le commissaire en poste ont formulé diverses recommandations visant à modifier la ***Loi sur la défense nationale***. Le commissaire est heureux que le gouvernement ait pris des mesures en vue de donner suite à ces recommandations.

APERÇU DES CONSTATATIONS ET RECOMMANDATIONS DE 2017–2018

Au cours de l'exercice 2017–2018, le commissaire a présenté au ministre huit rapports classifiés sur ses examens des activités du CST.

Les sept examens, ainsi qu'une étude, ont été menés sous l'autorité du commissaire :

- pour s'assurer que les activités du CST sont conformes à la loi, comme il est précisé à l'alinéa 273.63(2)a) de la *Loi sur la défense nationale*;
- pour contrôler la conformité des activités du CST menées sous le régime d'une autorisation ministérielle, comme l'établit le paragraphe 273.65(8) de la *Loi sur la défense nationale*.

Le bureau du commissaire a effectué un examen concernant une question pour laquelle un examen distinct a été jugé nécessaire à l'issue de l'examen effectué l'an dernier sur le partage de renseignements et les relations du CST avec des entités étrangères qui ne font pas partie de la Collectivité des cinq. Le bureau a examiné les pouvoirs du CST et sa participation à une initiative opérationnelle multilatérale.

Le bureau du commissaire a également terminé une étude de l'utilisation opérationnelle par le CST de plateformes internes de type média social afin d'acquérir des connaissances approfondies concernant ces activités et de déterminer tout problème pouvant nécessiter un examen de suivi.

Comme les années précédentes, le commissaire a effectué des examens annuels des autorisations ministérielles relatives à la collecte de renseignements électromagnétiques étrangers et à la cyberdéfense, notamment des vérifications ponctuelles des « communications canadiennes » (y compris les communications privées) qui ont été acquises, utilisées, conservées et détruites par le CST, ainsi que des incidents et des erreurs de procédure du CST liés à la vie privée. Le bureau a terminé les examens annuels des divulgations par le CST d'information sur l'identité de Canadiens pour 2015–2016 et 2016–2017. L'examen de 2015–2016 s'est poursuivi cette année.

RÉSULTATS

Chaque année, le commissaire présente une déclaration d'ensemble sur ses constatations concernant la légalité des activités du CST. ***Au cours de l'année écoulée, toutes les activités examinées étaient conformes à la loi.***

De même, cette année, le commissaire a formulé quatre recommandations pour promouvoir la conformité à la loi et renforcer la protection de la vie privée, demandant notamment que :

1. pour clarifier toute nouvelle activité liée au partage de renseignements avec des entités étrangères, le CST effectue des analyses adéquates en ce qui concerne les pouvoirs et les mesures de protection de la vie privée des Canadiens avant d'amorcer l'activité en question;
2. le CST prenne des mesures pour veiller à ce que toutes les demandes de divulgation d'information sur l'identité de Canadiens supprimée précisent le pouvoir légal en vertu duquel l'information est demandée et comportent une justification opérationnelle solide de la nécessité d'obtenir cette information qui est conforme au mandat de l'organisation présentant la demande;
3. le CST clarifie la terminologie employée dans ses autorisations ministérielles pour veiller à ce qu'elle reflète fidèlement la protection juridique reconnue et offerte relativement aux communications entre un conseiller juridique et son client dans le droit canadien, et pour assurer l'uniformité avec la terminologie utilisée dans ses politiques et pratiques relatives aux activités en matière de sécurité des technologies de l'information et aux activités de collecte de renseignements électromagnétiques étrangers;
4. le CST veille à ce que les mémoires de demande ultérieurs liés aux autorisations ministérielles contiennent de l'information détaillée de façon à décrire et à expliquer de manière exhaustive les activités de collecte de renseignements électromagnétiques étrangers envisagées par le CST, afin de mieux aider le ministre à prendre une décision.

POINTS SAILLANTS DES RAPPORTS PRÉSENTÉS AU MINISTRE EN 2017–2018

1. Examen des pouvoirs du CST et de sa participation à une initiative opérationnelle multilatérale

CONTEXTE

Au cours de l'examen du partage de renseignements du CST avec des entités étrangères mené l'an dernier, le bureau du commissaire a appris que le CST participait à une initiative opérationnelle multilatérale. Des questions ont été soulevées sur les pouvoirs en vertu desquels le CST participait à cette initiative ainsi que sur l'orientation, les politiques et le cadre opérationnel relatifs à sa participation. Pour ces raisons, le commissaire a décidé d'examiner cette activité de façon distincte.

L'examen constituait une occasion d'acquérir des connaissances approfondies sur la participation du CST à l'initiative multilatérale en vue de déterminer si les activités étaient conformes aux lois canadiennes et de vérifier que des mesures adéquates ont été prises pour protéger la vie privée des Canadiens. Le bureau du commissaire a examiné les activités, les rapports, les documents d'orientation et de politique ainsi que la correspondance interne liée à l'initiative pour la période allant de novembre 2013 à juin 2016.

Le CST entretient avec plusieurs entités étrangères des relations multilatérales de longue date qui impliquent la coopération et le partage de renseignements sur des questions d'intérêt mutuel. Le groupe multilatéral a récemment entrepris une initiative de collaboration visant l'élaboration de produits d'analyse fondés sur l'information partagée par les participants. À ce jour, l'initiative a été axée sur la menace terroriste posée par les voyageurs extrémistes, mais une forme de collaboration similaire pourrait servir d'autres intérêts communs.

Dans le cadre de l'initiative opérationnelle multilatérale, les participants collaborent à l'élaboration de produits d'analyse. L'information utilisée aux fins de l'analyse est fournie par les participants, qui l'acquièrent dans le cadre de leurs travaux de collecte indépendants relevant de leurs mandats juridiques respectifs. Grâce à sa participation à cette initiative, le CST peut consulter l'information partagée par les autres participants de même que les rapports d'analyse élaborés conjointement.

Plusieurs participants à l'initiative multilatérale ont des mandats de collecte de renseignements et sont assujettis à des limites qui sont prévus par leurs régimes juridiques et de politiques respectifs et diffèrent de ceux du CST.

Au titre du mandat de collecte de renseignements électromagnétiques étrangers du CST, dont il s'acquitte conformément à l'alinéa 273.64(1)a) de la ***Loi sur la défense nationale*** – partie a) du mandat du CST – les activités du CST ne peuvent viser des Canadiens et ces activités doivent être soumises à des mesures de protection de la vie privée des Canadiens – alinéas 273.64(2)a) et b). Lorsque le CST fournit une assistance technique et opérationnelle aux organismes fédéraux chargés de l'application de la loi et de la sécurité, dans l'exercice des fonctions que la loi leur confère, les activités du CST sont assujetties aux limites que la loi impose aux organismes en question, conformément à l'alinéa 273.64(1)c) de la ***Loi sur la défense nationale*** – partie c) du mandat du CST.

Si le Service canadien du renseignement de sécurité (SCRS) demande l'assistance du CST conformément à la partie c) de son mandat, ce dernier peut faire office de canal de transmission sûr de l'information provenant d'une entité étrangère qui pourrait être liée à une menace pour la sécurité du Canada, mais qui a pu être acquise par des activités visant un Canadien.

CONSTATATIONS ET RECOMMANDATION

Au début de l'examen, le bureau du commissaire a posé des questions sur les pouvoirs en vertu desquels le CST participait à l'initiative multilatérale, car il ne savait pas exactement si le CST participait à l'initiative au titre de son mandat de collecte de renseignements électromagnétiques étrangers ou au titre de son mandat d'assistance. Le bureau du commissaire a donc demandé au CST de confirmer les pouvoirs en vertu desquels il exerçait ses activités dans le cadre de l'initiative. Le CST maintient qu'il avait établi avant le début de l'activité qu'il allait participer à l'initiative au titre de son mandat de collecte de renseignements électromagnétiques étrangers. Toutefois, les documents internes examinés par le bureau du commissaire ont démontré que des discussions avaient eu lieu au sein du CST concernant la mesure dans laquelle les différentes parties de son mandat s'appliquaient, vu la possibilité que le CST reçoive de l'information sur des Canadiens ou de l'information obtenue grâce à des activités visant des Canadiens menées par les participants, et la façon dont de tels cas allaient être gérés. Rien ne permet au bureau du commissaire de penser qu'une décision ait été prise à cet égard, et c'est seulement plus tard au cours de l'examen que le CST a répondu explicitement aux questions concernant les pouvoirs applicables.

Avant de participer à l'initiative multilatérale et au tout début de sa participation, le CST n'a pas adéquatement documenté ses activités et il n'a ni pris de mesures correspondantes en ce qui concerne les pouvoirs déterminés (c.-à-d. le mandat

de collecte de renseignements électromagnétiques étrangers du CST), ni mis en œuvre de politiques.

Le bureau du commissaire a été informé que le CST n'avait obtenu aucun avis juridique précis concernant sa participation à l'initiative multilatérale. Le CST a toutefois pris en compte un avis juridique sur une question apparentée pour fournir des lignes directrices au cours des premières étapes.

Suite aux questions du bureau du commissaire concernant les pouvoirs en vertu desquels le CST participait à l'initiative multilatérale, le CST a obtenu un avis juridique précis sur le sujet et l'a communiqué au bureau du commissaire.

Pouvoirs

Le commissaire a constaté qu'au début de l'examen, le CST n'a pas clairement communiqué son approche en ce qui concerne sa participation à l'initiative multilatérale. Au lieu de planifier de façon explicite les modalités de sa participation, le CST a réagi aux nouveaux développements et s'est concentré sur la gestion du risque posé par la réception d'information obtenue grâce à des activités visant des Canadiens menées par les participants en vertu de leurs pouvoirs souverains. C'est seulement après un certain temps, au fil des expériences et avec du recul que le CST a établi que le risque posé par la réception d'information sur des Canadiens était faible.

En participant à l'initiative multilatérale au titre de son mandat de collecte de renseignements électromagnétiques étrangers, comme c'est le cas pour toute activité de collecte de renseignements électromagnétiques étrangers, le CST ne pouvait recevoir d'information obtenue grâce à des activités visant un Canadien et ses activités ne pouvaient viser un Canadien; de telles activités devraient également faire l'objet de mesures pour protéger la vie privée des Canadiens.

Chaque participant à l'initiative multilatérale exerce ses activités sous son propre régime juridique et de politiques. Il est donc possible qu'un participant choisisse de mener des activités de collecte visant un Canadien, s'il est dans son intérêt national de le faire. Lorsque les participants choisissent de partager de l'information, ils le font généralement en omettant la source de l'information et il est impossible de savoir comment l'information partagée a été acquise. Par conséquent, il est possible que l'information fournie par les participants dans le cadre d'une mission de lutte contre le terrorisme comprenne de l'information obtenue grâce à des activités de collecte visant un Canadien.

Le commissaire a jugé que les mesures de protection de la vie privée dont avaient convenu les participants et qu'ils avaient mises en place dans le cadre de l'initiative multilatérale étaient insatisfaisantes, puisqu'elles n'abordaient pas adéquatement la possibilité que le CST, sans le savoir, reçoive de l'information provenant d'un participant dont les activités visaient un Canadien au titre de son cadre national

juridique et de politiques. Cependant, à la lumière de l'information examinée, le commissaire n'a trouvé aucune indication de non-conformité à la loi. Le bureau du commissaire a examiné tous les rapports produits par l'équipe de l'initiative multilatérale au cours de la période visée par l'examen et n'a trouvé aucun cas où de l'information provenant des participants mettait en cause des Canadiens.

Si, au départ, l'initiative multilatérale avait pour objectif la collaboration d'organismes de collecte de renseignements électromagnétiques à des projets de lutte contre le terrorisme, l'intention énoncée consistait également à être prêt à intervenir en cas de crises ou de menaces. Or, les participants à l'initiative continuent d'axer leurs efforts sur les voyageurs extrémistes. Ce faisant, le CST court le risque, aussi faible soit-il, de recevoir sans le savoir de l'information découlant d'activités de collecte visant un Canadien menées par un autre participant au titre de son cadre national juridique et de politiques.

VOYAGEURS EXTRÉMISTES

On appelle « voyageur extrémiste » (ou « combattant étranger ») une personne soupçonnée de se rendre à l'étranger pour prendre part à des activités liées au terrorisme, par exemple les hommes et les femmes ayant quitté le Canada pour se joindre au groupe terroriste qui se fait appeler « État islamique ».

Orientation

Il est encourageant que, à la lumière de l'information examinée, il y avait des documents d'orientation et de politiques adéquats sur l'information sur les non-Canadiens que peut partager le CST avec les autres participants et sur les modalités du partage. Ces documents indiquent très clairement que le CST ne peut fournir aucune information sur un Canadien. Le commissaire n'a aucune préoccupation concernant ce que le CST partage avec les autres participants.

Le CST a également mis en place certaines mesures visant à protéger la vie privée des Canadiens en ce qui concerne l'utilisation de l'information reçue dans le cadre de l'initiative multilatérale. Le CST analyse les données reçues dans le cadre de l'initiative et, s'il détermine que celles-ci sont utiles, il rédige des rapports sur celles-ci et les distribue. Au besoin, le CST supprime des rapports toute information sur l'identité de Canadiens pour protéger la vie privée des Canadiens.

Toutefois, même si le CST a une politique en place concernant les activités menées dans le cadre de son mandat de collecte de renseignements électromagnétiques étrangers, le commissaire a relevé l'absence de politiques et d'orientation précises sur la participation du CST à cette initiative multilatérale en ce qui concerne

la possibilité de recevoir de l'information obtenue au moyen d'activités visant des Canadiens. L'orientation fournie aux employés du CST était informelle et portait essentiellement sur les efforts à déployer pour éviter que le CST ne s'expose à des situations où les autres participants mènent des activités visant un Canadien. L'information examinée par le bureau du commissaire donne à penser que le CST avait prévu fournir des documents aux autres participants à l'initiative pour préciser les limites auxquelles est assujetti le CST de par la loi et ses politiques. Le CST a été incapable de présenter un dossier démontrant que cela avait été fait. Au cours des dernières phases de l'examen, le CST a envoyé une pièce de correspondance aux autres participants à l'initiative multilatérale pour préciser les lignes directrices sur le plan juridique et sur celui des politiques du CST, rappelant précisément les limites prévues par la partie a) du mandat du CST et celles associées à la réception de l'information obtenue au moyen d'activités visant des Canadiens.

L'an dernier, lorsqu'il avait réalisé un examen du partage de renseignements du CST avec des entités étrangères, qui avait au départ soulevé des questions concernant la participation du CST à l'initiative multilatérale, le commissaire avait constaté que les ententes officielles conclues avec certaines entités étrangères énonçaient en des termes généraux seulement les mesures de protection de la vie privée des Canadiens au lieu de présenter explicitement les pouvoirs et les restrictions juridiques du CST, y compris le fait qu'au titre de son mandat de collecte de renseignements électromagnétiques étrangers, le CST ne peut pas recevoir d'information obtenue au moyen d'activités visant un Canadien. Le CST a répondu à ces constatations de façon positive pendant l'examen et a adressé des lettres à ces entités étrangères décrivant les pouvoirs et les restrictions juridiques du CST. Il s'agissait d'une mesure temporaire en attendant la modification des ententes. Le commissaire était satisfait de cette approche. Toutefois, il a encouragé le CST à modifier dès que possible toutes les ententes conclues avec des entités étrangères ou à conclure de nouvelles ententes, comme il l'avait recommandé dans le cadre de l'examen de l'an dernier sur le partage de renseignements avec des entités étrangères.

De plus, le commissaire **a recommandé** que, pour clarifier toute nouvelle activité liée au partage de renseignements avec des entités étrangères, le CST effectue des analyses adéquates en ce qui concerne les pouvoirs et les mesures de protection de la vie privée des Canadiens avant d'amorcer l'activité en question.

CONCLUSION

À la lumière de l'information examinée, le commissaire n'a trouvé aucune indication de non-conformité à la loi. Le commissaire comprend que la participation du CST à l'initiative multilatérale répond à une des grandes priorités du gouvernement du Canada, à savoir protéger les Canadiens contre la menace que représente le

terrorisme. Toutefois, il est également nécessaire de veiller à ce que les entités étrangères avec lesquelles traite le CST comprennent les limites juridiques auxquelles le CST est assujetti. Par conséquent, par suite de cet examen, le commissaire surveillera étroitement la mise en œuvre de la recommandation découlant de l'examen de l'an dernier sur le partage de renseignements avec des entités étrangères ainsi que la recommandation que renferme le présent rapport.

2. Étude sur l'utilisation opérationnelle par le CST de plateformes internes de type média social

CONTEXTE

Le bureau du commissaire a effectué une étude sur l'utilisation opérationnelle par le CST de plateformes internes de type média social pour la période allant du 1er janvier 2016 au 31 juillet 2017. Le CST a augmenté son utilisation de ces plateformes au cours des dernières années, principalement dans le but d'améliorer le partage de l'information et d'idées relatives aux opérations à l'interne et entre les partenaires de l'organisation.

Bien qu'elle soit avantageuse pour le CST et ses partenaires, l'utilisation de telles plateformes pourrait avoir des répercussions sur la vie privée des Canadiens et la conformité à la loi. Par conséquent, le bureau du commissaire a entrepris une étude en vue de prendre connaissance de la façon dont le CST utilise les plateformes internes de type média social dans un contexte opérationnel. L'étude doit permettre de mieux comprendre et d'évaluer les éventuelles répercussions sur la vie privée, de déterminer tout problème de conformité à la loi et d'en informer le commissaire. Le bureau du commissaire désirait également utiliser les connaissances acquises pour déceler toute question nécessitant un examen de suivi, et de façon générale, pour éclairer les examens futurs. L'étude a été effectuée en vertu des pouvoirs du commissaire prévus à l'alinéa 273.63(2)a) de la partie V.1 de la ***Loi sur la défense nationale***.

Les plateformes de type média social du CST comprennent des espaces collaboratifs virtuels (groupes) qui peuvent être créés pour permettre à des participants sélectionnés d'accéder à des répertoires d'information précis. Certains groupes sont uniquement à l'interne au CST, tandis que d'autres, appelés « groupes accessibles à l'externe », comprennent des participants d'autres organisations canadiennes ou étrangères. Il n'y a pas de rapports ou de liens entre les plateformes internes de type média social utilisées par le CST afin de partager de l'information et les médias sociaux utilisés par le public.

PLATEFORME INTERNE DE TYPE MÉDIA SOCIAL DU CST

Le CST a adopté une plateforme opérationnelle collaborative aux fins des opérations de mission (renseignements électromagnétiques étrangers et sécurité des technologies de l'information) qui permet au personnel des opérations de participer à des communautés d'intérêts, de partager de l'information et de collaborer à des projets liés aux opérations et aux missions. L'objectif ultime consiste à produire en temps opportun des produits du renseignement utiles et de grande qualité grâce à la collaboration au sein du CST et avec ses partenaires de la Collectivité des cinq et ceux des secteurs de la sécurité et du renseignement au Canada.

OBSERVATIONS

Politiques et contrôles

Le CST a mis en place des politiques et des directives écrites concernant l'utilisation des plateformes internes de type média social. Celles-ci portent notamment sur le respect de la vie privée et des lois et complètent d'autres politiques opérationnelles du CST d'application plus générale. Les activités qui font intervenir l'utilisation de plateformes internes de type média social doivent être conformes à toutes les politiques opérationnelles applicables. Cela comprend la conservation, l'utilisation et le partage de l'information sur l'identité de Canadiens. Sauf de rares exceptions, le partage d'information sur l'identité de Canadiens doit exclure les alliés et les organismes partenaires canadiens. Pendant la période visée par l'étude, aucune information sur l'identité de Canadiens n'a été communiquée à une entité étrangère ou à un organisme partenaire canadien par l'intermédiaire de ces plateformes.

Le CST a également élaboré un régime d'approbation et de surveillance de la conformité concernant l'utilisation de ces plateformes. Ce régime comprend des gestionnaires hiérarchiques opérationnels et des équipes d'examen internes chargés de veiller à ce que les approbations, les accès, le contenu, le partage et la conservation des données ainsi que la formation soient adéquats.

Culture de protection de la vie privée et sensibilisation

La culture de protection de la vie privée du CST transparaissait dans les connaissances et les pratiques en matière de protection de la vie privée des présentateurs du CST et des personnes interrogées pendant l'étude, y compris pendant les démonstrations de la plateforme et le traitement de l'information sur l'identité de Canadiens contenue dans celle-ci. Cette culture se traduisait également dans

les instruments de politique et les directives élaborées et mises en œuvre expressément aux fins de l'utilisation opérationnelle de plateformes de type média social, les exigences relatives aux accès et les limites programmées dans ces plateformes, la collecte de données sur l'utilisation de la plateforme et le suivi connexe ainsi que les régimes de surveillance de la conformité et de production de rapports en place.

Formation

Une formation sur l'utilisation des plateformes internes de type média social du CST est fournie aux employés du CST et, s'il y a lieu, aux participants externes. Cette formation semble être adéquate; toutefois, un examen interne du CST effectué en 2017 a permis de constater que moins de la moitié des responsables de groupes accessibles à l'externe avaient suivi la formation requise. Le CST a avisé le bureau qu'il était en train de résoudre ce problème.

Assurance de la conformité interne et gestion de l'information

Les équipes de la conformité des secteurs du CST responsables des renseignements électromagnétiques étrangers et de la sécurité des technologies de l'information surveillent l'utilisation des plateformes internes de type média social du CST pour s'assurer qu'elle est conforme aux politiques, aux pouvoirs et aux directives du CST. Par exemple, pendant la période visée par l'étude, l'équipe de la conformité de la sécurité des technologies de l'information du CST a vérifié qu'aucune donnée de cyberdéfense n'ayant pas fait l'objet d'une évaluation ne se trouvait sur ces plateformes, puisque ce type de données n'est pas permis sur ces plateformes. Au cours de la vérification, un cas de données n'ayant pas fait l'objet d'une évaluation a été décelé. L'équipe de la conformité a donc rappelé la politique en diffusant un communiqué sur l'utilisation acceptable des plateformes internes de type média social.

L'équipe de la conformité du secteur responsable des renseignements électromagnétiques étrangers a également entrepris deux examens pendant la même période. Même si les examens internes n'ont soulevé aucune préoccupation relative au contenu ou au respect de la vie privée, l'équipe a trouvé que 19 pour cent des groupes actifs accessibles à l'externe n'avaient pas consigné correctement les approbations requises pour la mise sur pied du groupe et qu'à plusieurs reprises, un responsable d'un groupe accessible à l'externe avait été remplacé sans que le changement soit signalé, même s'il est nécessaire de le faire. L'équipe de la conformité a recommandé que les approbations et le remplacement du responsable soient documentés de façon centrale et uniforme à des fins de surveillance et d'examen. (L'équipe de la conformité du secteur responsable des renseignements électromagnétiques étrangers a également formulé une recommandation relative

aux lacunes susmentionnées concernant la formation.) Le CST a indiqué que ces recommandations ont été acceptées et mises en œuvre.

Dans le cadre du processus de surveillance de la conformité, les gestionnaires responsables des renseignements électromagnétiques étrangers vérifient chaque année que tous les fonds d'information sur l'identité de Canadiens, y compris les plateformes internes de type média social, sont valides et continuent d'être requis. Dans le contexte de l'étude, le bureau du commissaire a trouvé des incohérences dans la façon dont les formulaires étaient remplis. Le bureau a également constaté qu'en date de novembre 2017, les formulaires les plus récents remontaient à juillet 2016. Le bureau du commissaire s'attendait à ce que les responsables des renseignements électromagnétiques étrangers aient examiné leurs fonds d'information depuis cette date, conformément à leur propre politique. Le CST a signalé que l'examen de la conformité de 2017 en lien avec l'information sur l'identité de Canadiens avait commencé en novembre 2017 et qu'il a pris des mesures correctives.

Un groupe interne de média social a été mis sur pied pour contribuer à une affaire opérationnelle hautement prioritaire. Une fois l'affaire close avec succès, le groupe interne de média social, qui contenait de l'information relative à la vie privée de Canadiens, est demeuré ouvert pendant plus de 15 mois et accessible à tous les employés opérationnels du CST ayant un compte sur cette plateforme. Le CST a expliqué l'utilité de ne pas fermer ce groupe en particulier. Toutefois, le bureau du commissaire se demande pourquoi le groupe doit demeurer actif si longtemps après la fin de l'opération et pourquoi ce genre d'information potentiellement délicate demeure largement accessible. Selon la politique du CST, l'information se trouvant sur les plateformes internes de type média social est considérée comme transitoire et elle doit être supprimée lorsqu'elle n'est plus requise, tout particulièrement l'information sur l'identité de Canadiens et l'information relative à la vie privée de Canadiens. Conformément à la politique du CST, l'information qui présente une valeur opérationnelle doit être conservée dans le répertoire organisationnel officiel du CST.

Le CST a diffusé des instructions sur la gestion des dossiers dans le contexte des plateformes internes de type média social ainsi que des instructions plus générales. Malgré cela, le bureau du commissaire a examiné, pendant l'étude, des documents constituant des instruments de politique officiels du CST qui ne précisaient aucune date d'entrée en vigueur (ou aucune date) et qui n'étaient pas identifiés comme étant des documents officiels. Même si le CST a indiqué que ces instruments de politique peuvent être consultés par les personnes qui en ont besoin, il est important de souligner que les précisions offertes par cette information aident les opérations en facilitant la gestion des versions et en faisant en sorte que les employés participant à la mission reçoivent des instructions à jour et sans ambiguïté. Une gestion des dossiers rigoureuse est également

essentielle à l'efficacité de la surveillance de la conformité, des vérifications et des examens.

CONCLUSION

L'étude a permis de constater que le CST dispose d'un ensemble de politiques adéquat pour régir l'utilisation opérationnelle des plateformes internes de type média social, même si certaines des politiques stratégiques écrites du CST examinées ne précisaient aucune date d'entrée en vigueur et n'indiquaient pas clairement qu'elles constituaient des documents officiels. Ces problèmes peuvent rendre les politiques moins efficaces en ce qui concerne la fourniture d'une orientation claire et sans ambiguïté aux employés et l'exécution efficace d'activités de surveillance de la conformité, de vérifications et d'examens. De plus, le CST favorise une culture de la conformité en ce qui concerne la protection de la vie privée relativement à l'utilisation des plateformes internes de type média social et, à l'exception des lacunes concernant la formation de certains utilisateurs, le modèle de formation des utilisateurs semble être adéquat, car les employés du CST sont bien renseignés et soucieux de protéger la vie privée des Canadiens lorsqu'ils utilisent ces plateformes à des fins opérationnelles. Le commissaire surveillera les préoccupations soulevées dans l'étude et déterminera si un examen de suivi est nécessaire à cet égard.

3. Examen annuel des divulgations d'information sur l'identité de Canadiens par le CST, 2015–2016

CONTEXTE

Chaque année, le bureau du commissaire examine un échantillon des divulgations d'information sur l'identité de Canadiens par le CST. Cela comprend toute information concernant un Canadien ou pouvant être utilisée pour identifier un Canadien. L'examen des divulgations faites en 2015–2016 s'est achevé après le 31 mars 2017, et c'est pourquoi il en est fait état cette année. L'objectif de l'examen consistait à vérifier si le CST, dans ses divulgations d'information sur l'identité de Canadiens, était conforme à la loi, aux instructions ministérielles et à ses politiques et procédures. La mesure dans laquelle le CST a protégé la vie privée des Canadiens a également été évaluée.

Au titre de son mandat de collecte de renseignements électromagnétiques étrangers, le CST doit « acquérir et utiliser l'information provenant de l'infrastructure mondiale d'information dans le but de fournir des renseignements étrangers »

(alinéa 273.64(1)a) de la *Loi sur la défense nationale*). Ces activités ne peuvent viser des Canadiens ou toute personne au Canada et elles doivent être soumises à des mesures de protection de la vie privée des Canadiens lors de l'utilisation et de la conservation des renseignements interceptés (alinéas 273.64(2)a) et b) de la *Loi sur la défense nationale*).

Même si la *Loi sur la défense nationale* ne confère pas au CST le pouvoir explicite de divulguer de l'information sur l'identité de Canadiens, y compris des renseignements personnels, il est entendu que ce pouvoir découle implicitement du mandat de collecte de renseignements électromagnétiques étrangers du CST. Les commissaires, y compris le commissaire en poste, ont recommandé que la *Loi sur la défense nationale* soit modifiée en vue d'accorder au CST le pouvoir explicite de recueillir, d'utiliser et de divulguer de l'information sur des Canadiens obtenue fortuitement dans le cadre d'activités prévues par son mandat. (La question semble avoir été abordée dans le projet de loi C-59 du gouvernement, la *Loi concernant des questions de sécurité nationale*.)

Lorsqu'il recueille des renseignements électromagnétiques étrangers à l'appui des priorités en matière de renseignement du gouvernement du Canada, le CST peut obtenir de manière non intentionnelle de l'information sur l'identité de Canadiens ou de l'information sur des Canadiens. Si l'information est utilisée dans un rapport, toute information sur l'identité de Canadiens (noms, numéros de téléphone, adresses de protocole Internet, numéros de passeport et tout autre renseignement pouvant révéler l'identité d'une personne ou d'une société canadienne) doit être supprimée et remplacée par une mention générique. De plus, les rapports sur les renseignements étrangers du CST peuvent seulement inclure des références à des Canadiens si ces dernières sont essentielles à la compréhension des renseignements étrangers.

Lorsque le CST produit un rapport sur les renseignements étrangers où de l'information sur l'identité de Canadiens a été supprimée, les clients du CST pouvant démontrer qu'ils ont le pouvoir légal et le besoin opérationnel de recevoir de l'information sur l'identité de Canadiens peuvent présenter une demande de divulgation de l'information. Une fois la demande évaluée, le CST peut divulguer l'information sur l'identité de Canadiens en vertu de l'alinéa 273.64(1)a) de la *Loi sur la défense nationale* et, en ce qui concerne les renseignements personnels, en vertu du paragraphe 8(2) de la *Loi sur la protection des renseignements personnels*.

Le pouvoir du CST de divulguer de l'information sur l'identité de Canadiens qui a été supprimée dépend du pouvoir du client de recueillir cette information sur l'identité de Canadiens. La divulgation d'information sur l'identité de Canadiens doit être effectuée conformément à la *Loi sur la défense nationale*, à la *Loi sur la protection des renseignements personnels* et au cadre de la politique opérationnelle du CST, qui reconnaît que le client qui reçoit l'information doit justifier son droit de la recevoir. Lorsque des renseignements personnels doivent être divulgués,

le CST doit être convaincu que le demandeur recueille l'information à des fins qui ont un lien direct avec ses programmes ou ses activités (article 4 de la ***Loi sur la protection des renseignements personnels***) et que les renseignements sont demandés à des fins de renseignements étrangers conformes aux priorités du gouvernement du Canada en matière de renseignement ou à des fins compatibles. Si la demande de divulgation de l'information sur l'identité de Canadiens supprimée dépasse la portée du mandat de collecte de renseignements électromagnétiques étrangers, d'autres circonstances décrites au paragraphe 8(2) de la ***Loi sur la protection des renseignements personnels*** pourraient permettre la divulgation de l'information.

Aux fins de l'examen, le bureau du commissaire a sélectionné et examiné un échantillon correspondant à environ 20 pour cent (243 demandes au départ) des 1 211 demandes de divulgation d'information sur l'identité de Canadiens contenue dans des rapports du CST présentées par des clients du CST au sein du gouvernement du Canada.

Les demandes examinées ont été reçues par le CST entre le 1er juillet 2015 et le 30 juin 2016. Toutes les institutions gouvernementales qui ont présenté une demande de divulgation d'information sur l'identité de Canadiens pendant cette période ont été représentées dans l'échantillon. Lorsqu'il était devenu clair qu'un client donné du gouvernement du Canada présentait des demandes qui ne comportaient pas suffisamment de détails, l'échantillon a été élargi et porté à 249 demandes afin d'inclure l'ensemble des 27 demandes présentées par ce client.

Le bureau a également examiné chacune des 100 demandes provenant d'alliés et des cinq demandes présentées par un client du gouvernement du Canada qui visaient la divulgation d'information sur l'identité de Canadiens à des entités ne faisant pas partie de la Collectivité des cinq. Le CST a la responsabilité de réaliser une évaluation du risque de mauvais traitements lorsqu'il divulgue de l'information. Toutefois, les autres institutions du gouvernement du Canada continuent d'être responsables de la réalisation d'évaluations du risque de mauvais traitements lorsqu'ils partagent l'information par leurs propres canaux de communication. Dans les divulgations à des destinataires autres que les partenaires de la Collectivité des cinq, le CST inclut une mise en garde précise visant à rappeler au client gouvernemental demandeur sa responsabilité d'effectuer une évaluation des risques associés au partage de renseignements avec une entité étrangère.

PARTENAIRES DE LA COLLECTIVITE DES CINQ (*FIVE EYES*)
Les partenaires de la Collectivité des cinq sont le CST et les principaux organismes internationaux des pays de la Collectivité des cinq : la National Security Agency des États-Unis, le Government Communications Headquarters du Royaume-Uni, l'Australian Signals Directorate et le Government Communications Security Bureau de la Nouvelle-Zélande. Ce groupe est également connu sous le terme d'« alliés ».

Le nombre de divulgations d'information sur l'identité de Canadiens est fondé sur la méthode de dénombrement du CST. Le nombre de demandes correspond au nombre de fois où des institutions ou des partenaires ont présenté des demandes distinctes de divulgation d'information sur l'identité supprimée dans des rapports en fournissant une justification opérationnelle distincte dans chaque cas. Une demande pouvait comprendre de multiples identités canadiennes et une identité canadienne pouvait être divulguée à plusieurs reprises à différentes institutions ou à différents partenaires.

CONSTATATIONS ET RECOMMANDATION

Le commissaire a jugé que les divulgations par le CST d'information sur l'identité de Canadiens, y compris les divulgations aux alliés ou les divulgations par un client du gouvernement du Canada à une entité ne faisant pas partie de la Collectivité des cinq, étaient conformes à la loi et aux instructions ministérielles concernant la protection de la vie privée des Canadiens.

Le CST a apporté une modification technique visant à mettre à niveau le système utilisé pour traiter les demandes d'information sur l'identité de Canadiens provenant de clients du gouvernement du Canada; la demande de divulgation initiale et le refus sont maintenant consignés dans le système. La demande initiale n'était pas incluse auparavant.

Pour ce qui est de la façon dont le CST divulgue l'information sur l'identité de Canadiens à des clients du gouvernement du Canada, le commissaire a constaté une occasion pour le CST de renforcer ses procédures afin d'être plus diligent lorsqu'il examine la justification opérationnelle fournie. Une telle approche pourrait contribuer à l'application par le CST de mesures satisfaisantes en vue de protéger l'information sur l'identité de Canadiens et la vie privée des Canadiens, conformément à la ***Loi sur la défense nationale*** et à la ***Loi sur la protection des renseignements personnels***.

Après avoir examiné les documents pertinents, le bureau du commissaire a fait part de ses préoccupations aux employés et aux gestionnaires du CST responsables des politiques, aux cadres supérieurs du CST et au conseiller juridique de

Justice Canada au CST relativement à huit demandes provenant du même client dans lesquelles il manquait la description explicite des pouvoirs précis et les justifications opérationnelles. Même si le commissaire a établi que le client du gouvernement du Canada avait le pouvoir légal de recueillir de l'information sur l'identité de Canadiens dans ces cas, le CST a divulgué l'information sans avoir obtenu suffisamment de précisions de la part du client pour pouvoir corroborer son pouvoir légal de recueillir de l'information sur l'identité de Canadiens et sans avoir obtenu de justification opérationnelle adéquate montrant que la collecte d'information sur l'identité de Canadiens par le client avait un lien direct avec l'un de ses programmes. Le commissaire a déterminé que le processus de divulgation du CST n'était pas suffisamment rigoureux et que le CST n'avait pas fait preuve de la diligence nécessaire dans ces cas. La politique du CST n'oblige pas le client à nommer une loi précise en guise d'autorisation de recevoir des renseignements; il suffit au client de fournir une justification solide de la demande qui décrit les besoins du client en ce qui concerne l'information supprimée, qui explique la façon dont l'information est liée à son mandat et à son programme et qui confirme que les renseignements demeureront sous le contrôle du demandeur.

Le CST a reconnu que les justifications fournies par le client au départ ne renfermaient pas les précisions voulues.

Le commissaire **a recommandé** que le CST prenne des mesures pour veiller à ce que toutes les demandes de divulgation d'information sur l'identité de Canadiens supprimée précisent le pouvoir légal en vertu duquel l'information est demandée et comportent une justification opérationnelle solide de la nécessité d'obtenir cette information qui est conforme au mandat de l'organisation présentant la demande. Le commissaire s'attend à ce que des éléments probants lui soient présentés montrant que le CST prend des mesures pour donner suite à la recommandation au cours de son examen des divulgations par le CST de l'information sur l'identité de Canadiens en 2017–2018.

CONCLUSION

Pour régler les problèmes cernés dans le cadre de cet examen, le CST a déjà fourni des instructions à l'équipe responsable des divulgations d'information sur l'identité de Canadiens pour assurer un examen minutieux des demandes futures. De plus, le CST a temporairement suspendu (sauf en cas d'urgence) les divulgations au client du gouvernement du Canada dont les demandes ne contenaient pas suffisamment de détails. Par la suite, le CST a modifié ses procédures afin d'être plus diligent lorsqu'il étudie les justifications fournies par ce client du gouvernement du Canada en vue d'obtenir de l'information sur l'identité de Canadiens et il réexamine les exigences en matière de renseignements que les clients doivent fournir lorsqu'ils demandent de l'information sur l'identité de Canadiens. Enfin, le CST a modifié la procédure en vue d'exiger une approbation de niveau supérieur

pour les demandes d'information sur l'identité de Canadiens provenant de ce client du gouvernement du Canada. Il s'agit de changements positifs.

Depuis l'examen de 2014–2015, le CST a modifié ses politiques en ce qui concerne les niveaux d'approbation. Le CST a réduit le niveau d'approbation requis pour autoriser la divulgation d'information sur l'identité de Canadiens dans trois autres cas précis. Selon le CST, le changement a réglé un problème relatif à des pouvoirs d'approbation inutilement élevés qui retardaient la communication de l'information aux clients du CST. Les répercussions de ces modifications apportées aux politiques n'ont pas été remarquées. Toutefois, le commissaire surveillera le changement dans ses examens futurs.

4. Examen annuel des divulgations d'information sur l'identité de Canadiens par le CST, 2016–2017

CONTEXTE

Il s'agit du neuvième examen annuel consécutif d'un échantillon des divulgations d'information sur l'identité de Canadiens par le CST. L'objectif des examens annuels demeure le même : vérifier si le CST, dans ses divulgations d'information sur l'identité de Canadiens, était conforme à la loi, aux instructions ministérielles et à ses politiques et procédures. La mesure dans laquelle le CST a protégé la vie privée des Canadiens a également été évaluée.

DIVULGATION D'INFORMATION SUR L'IDENTITÉ DE CANADIENS

L'information pouvant permettre d'identifier un Canadien est habituellement supprimée, c'est-à-dire remplacée par une mention générale telle que « Canadien nommé », afin de protéger l'identité de cette personne. Les clients du CST au sein du gouvernement du Canada et les alliés peuvent demander et recevoir cette information s'ils ont les pouvoirs de les recevoir et une justification opérationnelle adéquate. La divulgation d'information sur l'identité de Canadiens doit être effectuée conformément à la *Loi sur la protection des renseignements personnels* et au cadre de la politique opérationnelle du CST. Pour en apprendre davantage sur les pouvoirs et les limites se rapportant aux activités du CST, veuillez consulter le site Web du bureau.

Cette année, le bureau du commissaire a sélectionné et examiné un échantillon correspondant à 22 pour cent (236 demandes) des 1 067 demandes de divulgation d'information sur l'identité de Canadiens contenue dans des rapports du CST présentées par des clients du CST au sein du gouvernement du Canada. L'examen portait sur les demandes reçues par le CST entre le 1er juillet 2016 et le 30 juin 2017. Toutes les institutions gouvernementales qui ont présenté une demande de divulgation d'information sur l'identité de Canadiens pendant cette période ont été représentées dans l'échantillon. De plus, l'échantillon comprenait toutes les demandes présentées par un client du gouvernement du Canada identifié dans l'examen de 2015–2016, car ses demandes d'information sur l'identité de Canadiens ne comportaient pas suffisamment de détails.

Le bureau a également examiné chacune des 62 demandes provenant d'alliés et des sept demandes présentées par deux clients du gouvernement du Canada qui visaient la divulgation d'information sur l'identité de Canadiens à des entités ne faisant pas partie de la Collectivité des cinq. Le CST a la responsabilité de réaliser une évaluation du risque de mauvais traitements lorsqu'il divulgue de l'information. Toutefois, les autres institutions du gouvernement du Canada continuent d'être responsables de la réalisation d'évaluations du risque de mauvais traitements lorsqu'ils partagent l'information par leurs propres canaux de communication. Dans les divulgations à des destinataires autres que les partenaires de la Collectivité des cinq, le CST inclut une mise en garde précise visant à rappeler au client gouvernemental demandeur sa responsabilité d'effectuer une évaluation des risques associés au partage de renseignements avec une entité étrangère.

Au cours de l'examen, le CST n'a pas été en mesure de fournir des copies de trois rapports de produits d'analyse dans leur version originale diffusée au moment de la divulgation de l'information sur l'identité de Canadiens, puisqu'après la divulgation, ces rapports ont été annulés ou modifiés. Le bureau du commissaire comprend que cette pratique est conforme à la politique du CST et constitue une mesure de protection de la vie privée des Canadiens. Toutefois, le bureau n'a pas été en mesure d'évaluer la conformité en ce qui touche ces cas précis de divulgation d'information sur l'identité de Canadiens. Le bureau du commissaire n'a aucune raison de croire que ces cas n'ont pas été gérés de la même façon que les autres cas examinés.

CONSTATATIONS

Le commissaire s'est dit convaincu de ce qui suit :

- les divulgations par le CST d'information sur l'identité de Canadiens étaient conformes à la loi;
- le client du gouvernement du Canada ou l'allié qui a présenté la demande avait à la fois le pouvoir et la justification opérationnelle requis pour obtenir l'information;

- le CST a appliqué efficacement les mesures de protection de la vie privée mentionnées dans les instructions ministérielles ainsi que dans ses politiques et procédures opérationnelles; et
- le CST a respecté le cadre établi par le Cabinet concernant les risques inhérents au partage de l'information avec des entités étrangères susceptible d'entraîner des mauvais traitements.

En janvier 2018, le commissaire a présenté au ministre de la Défense nationale les résultats de son examen des divulgations par le CST de l'information sur l'identité de Canadiens pour 2015–2016. Le rapport recommandait notamment au CST de renforcer ses procédures afin d'être plus diligent et de s'assurer que toutes les demandes de divulgation d'information sur l'identité de Canadiens précisent le pouvoir légal en vertu duquel les renseignements sont demandés et comportent une justification opérationnelle solide de la nécessité d'obtenir ces renseignements qui est conforme au mandat du demandeur. Le commissaire s'attend à ce que des éléments probants lui soient présentés montrant que le CST prend des mesures pour donner suite à la recommandation au cours de son examen des divulgations par le CST de l'information sur l'identité de Canadiens en 2017–2018. Dans le cadre de l'examen de cette année, le bureau du commissaire a mené une analyse comparative des demandes de divulgation provenant de divers clients au sein du gouvernement du Canada et il a relevé des cas où le pouvoir légal ou la justification opérationnelle appuyant la demande de divulgation d'information sur l'identité de Canadiens pouvait être renforcé. Ces cas concernaient non seulement le client du gouvernement du Canada identifié dans l'examen de 2015–2016 parce qu'il ne fournissait pas suffisamment de détails dans ses demandes, mais aussi quelques autres clients du gouvernement du Canada.

Le 17 octobre 2017, les instructions ministérielles intitulées ***Éviter la complicité dans les cas de mauvais traitements par des entités étrangères*** ont remplacé les instructions ministérielles de 2011 intitulées ***Cadre de gestion des risques liés au partage de renseignements avec des entités étrangères***. Même si la mise en œuvre des nouvelles instructions ministérielles n'a pas eu lieu pendant la période visée par l'examen, elle sera surveillée dans le cadre de l'examen sur la divulgation d'information sur l'identité de Canadiens de l'année prochaine.

Depuis l'examen de 2015–2016, le CST n'a ni modifié ses politiques ni apporté de changements techniques à son processus de divulgation d'information sur l'identité de Canadiens. Bien que le CST ait signalé au cours d'examens antérieurs qu'il évaluait des options visant à automatiser le processus de divulgation d'information sur l'identité de Canadiens aux alliés, aucun changement technique du genre n'a été effectué pendant la période visée par l'examen.

CONCLUSION

L'examen n'a débouché sur aucune recommandation.

Une question a été soulevée et fait l'objet d'un examen distinct afin que les résultats de l'examen de 2016–2017 puissent être présentés au ministre avant la fin de l'exercice. Lors de l'approbation d'une demande d'un client du gouvernement du Canada concernant de l'information sur l'identité d'un Canadien, une activité d'analyse des métadonnées du CST a soulevé des préoccupations. L'examen distinct était en cours en date du 31 mars 2018.

Le bureau continuera d'effectuer des examens annuels des divulgations par le CST d'information sur l'identité de Canadiens à des clients et à des partenaires pour vérifier si le CST se conforme à la loi et protège la vie privée des Canadiens.

5. Examen annuel des activités de cyberdéfense du CST menées sous le régime d'une autorisation ministérielle, 2016–2017

CONTEXTE

Le CST mène des activités de cyberdéfense sous le régime de l'alinéa 273.64(1)b) de la ***Loi sur la défense nationale*** – partie b) de son mandat. Cette partie du mandat autorise le CST à aider à protéger les renseignements électroniques et les infrastructures d'information importantes pour le gouvernement du Canada, ce qui est communément appelé la sécurité des technologies de l'information (TI). Les activités menées dans le cadre de la partie b) du mandat du CST ne doivent pas viser des Canadiens, où qu'ils se trouvent, ou toute personne au Canada et elles doivent faire l'objet de mesures pour protéger la vie privée des Canadiens en ce qui a trait à l'utilisation et à la conservation des renseignements interceptés [alinéas 273.64(2)a) et b) de la ***Loi sur la défense nationale***].

Les activités de cyberdéfense consistent à détecter et à contrer les cybermenaces sophistiquées. À la réception d'une demande écrite d'une institution du gouvernement du Canada en vue de la conduite d'activités de cyberdéfense, le CST peut déployer des mesures pour recueillir et analyser des données du système ou du réseau de ce client. Étant donné que les activités de cyberdéfense pourraient entraîner l'interception de communications privées, le CST doit mener ces activités sous le régime d'une autorisation ministérielle. Aux termes du paragraphe 273.65(3) de la ***Loi sur la défense nationale***, le ministre peut – dans le seul but de protéger les systèmes ou les réseaux informatiques du gouvernement du Canada contre les cybermenaces – autoriser par écrit le CST à intercepter des communications

privées qui sont liées à une activité ou une catégorie d'activités qu'il mentionne expressément. Dans le cadre des activités de cyberdéfense, les données interceptées par le CST, y compris les communications privées, peuvent être utilisées ou conservées seulement si l'interception était pertinente et nécessaire pour identifier, isoler ou prévenir les activités dommageables visant les systèmes ou les réseaux informatiques du gouvernement du Canada.

AUTORISATIONS MINISTÉRIELLES

Les autorisations ministérielles permettent au CST de passer outre l'interdiction d'intercepter des communications privées énoncée à la partie VI du *Code criminel*. Il s'agit d'un document écrit en vertu duquel le ministre de la Défense nationale autorise le CST à entreprendre une activité ou une catégorie d'activités comportant un risque d'interception non intentionnelle de communications privées. Les autorisations ne peuvent demeurer en vigueur pendant une période de plus d'un an. Pour en apprendre davantage sur les autorisations et les limites imposées aux activités du CST, veuillez consulter le site Web du bureau.

L'examen a porté sur l'autorisation ministérielle relative aux activités de cyberdéfense en vigueur du 1er juillet 2016 au 30 juin 2017. L'objectif de l'examen était d'évaluer la conformité à la loi des activités de cyberdéfense du CST, ainsi que la mesure dans laquelle le CST protège la vie privée des Canadiens. Dans le cadre de cet examen, le bureau du commissaire a examiné les mémoires de demande adressés au ministre de la Défense nationale relativement aux autorisations ministérielles de 2014–2015, 2015–2016 et 2016–2017 du CST, les autorisations ministérielles connexes de même que le rapport du CST de fin d'exercice présenté au ministre sur les autorisations ministérielles de 2016–2017. Le bureau a reçu des séances d'information sur place, mené des entrevues et examiné les bases de données et les systèmes du CST ainsi que divers types de rapports, tant internes qu'externes. Le bureau a sélectionné, aux fins de l'examen, un échantillon correspondant à 36 pour cent des incidents cybernétiques, lequel comprenait des communications privées.

CONSTATATIONS ET RECOMMANDATION

Le commissaire a conclu que l'autorisation ministérielle de cyberdéfense de 2016–2017 respectait les conditions d'autorisation énoncées dans la ***Loi sur la défense nationale***. Le CST n'a apporté aucun changement important à l'autorisation ministérielle ou à la façon dont les activités de cyberdéfense sont menées qui aurait présenté un risque pour la conformité à la loi ou la protection de la vie privée. Au

cours de la période visée par l'examen, aucune modification importante n'a été apportée aux instruments de politique régissant les activités de cyberdéfense menées sous le régime d'une autorisation ministérielle. Il n'y avait aucune donnée probante selon laquelle le CST aurait mené des activités de cyberdéfense qui seraient contraires aux exigences législatives, ministérielles ou des politiques. En se fondant sur un examen des communications privées identifiées que le CST a interceptées, le commissaire a conclu que le CST n'avait pas visé, au moyen de ses activités de cyberdéfense, des Canadiens ou toute personne au Canada. La majorité des communications privées examinées se rapportaient à une activité ou à un trafic malveillant et à des anomalies suspectes dans le contexte de la détection des cybermenaces. Les communications privées conservées et utilisées dans des rapports étaient essentielles pour identifier, isoler ou prévenir les activités dommageables visant les systèmes ou les réseaux informatiques du gouvernement du Canada.

Définition des communications entre un conseiller juridique et son client

Le commissaire a formulé une recommandation à la lumière d'un changement dans la terminologie utilisée par le CST dans l'autorisation ministérielle de cyberdéfense en ce qui concerne les communications entre un conseiller juridique et son client. L'autorisation ministérielle précise les mesures à prendre quand un analyste du CST identifie une communication entre un client et un « conseiller juridique canadien ». Le bureau du commissaire a demandé une explication au CST relativement à l'ajout du qualificatif « canadien », lequel ne figurait pas explicitement dans les autorisations ministérielles antérieures. Le CST a fait savoir que le qualificatif « canadien » n'était pas nouveau et qu'il avait été intégré dans l'autorisation ministérielle dans un souci de clarté. Toutefois, le commissaire a conclu que l'intégration de ce qualificatif créait une ambiguïté. De plus, le fait de préciser qu'il s'agit d'une communication entre un client et un conseiller juridique canadien a pour conséquence que l'autorisation ministérielle ne cadre pas avec les politiques et les pratiques du CST.

Selon la définition du terme « Canadien » au sens de la ***Loi sur la défense nationale***, ce terme évoque la citoyenneté – en désignant un citoyen canadien, un résident permanent ou une personne morale constituée au Canada – sans égard au lieu. Le commissaire s'attend à ce que les termes employés dans les autorisations ministérielles soient conformes aux définitions prévues par la ***Loi sur la défense nationale***. Cependant, le CST a fait savoir que, dans la pratique, il se fonde sur la définition d'une communication entre un conseiller juridique et son client qui se trouve dans sa politique générale sur la protection de la vie privée, laquelle ne comprend pas le terme « canadien » et ne fait pas mention de la citoyenneté ni du lieu géographique. La définition repose plutôt sur la question de savoir si la personne est autorisée à pratiquer le droit au Canada. Ainsi, lorsque des

communications entre un conseiller juridique et son client sont interceptées, le CST doit non seulement établir si le conseiller juridique est « canadien », mais également où se trouve le conseiller juridique (au Canada ou à l'étranger) et s'il est autorisé à pratiquer le droit au Canada.

En examinant l'instrument de politique général du CST sur la protection de la vie privée, le bureau du commissaire a remarqué que la définition d'une communication entre un conseiller juridique et son client ne vise que le traitement de telles communications dans le cadre des mandats du CST en matière de renseignements électromagnétiques étrangers et d'assistance – elle ne s'applique pas explicitement au mandat du CST en matière de sécurité des TI. Une autre politique portant expressément sur le mandat du CST en matière de sécurité des TI comprend une section sur les communications entre un conseiller juridique et son client; cependant, le terme « conseiller juridique canadien » n'y figure pas, et les communications entre un conseiller juridique et son client n'y sont pas définies. En outre, les directives concernant le traitement d'une communication entre un conseiller juridique et son client contenues dans cette politique ne sont pas claires sur le plan de la procédure. Le CST a fait savoir qu'il a depuis modifié la politique. Le bureau du commissaire évaluera les modifications en question dans le cadre de l'examen de l'année prochaine.

Le commissaire estime qu'il y a un manque d'uniformité entre la définition d'une communication entre un conseiller juridique et son client qui se trouve dans les autorisations ministérielles relatives aux activités de cyberdéfense et aux renseignements électromagnétiques étrangers, l'application du concept dans les pratiques du CST, et ce qui figure dans la politique sur la sécurité des TI. Par conséquent, le commissaire **a recommandé** que le CST clarifie la terminologie employée dans ses autorisations ministérielles pour veiller à ce qu'elle reflète fidèlement la protection juridique reconnue et offerte relativement aux communications entre un conseiller juridique et son client dans le droit canadien, et pour assurer l'uniformité avec la terminologie utilisée dans ses politiques et pratiques relatives aux activités en matière de sécurité des TI et aux activités de collecte de renseignements électromagnétiques étrangers. Le commissaire surveillera ce qui sera accompli à cet égard.

Communications privées de cyberdéfense

Le bureau du commissaire a sélectionné et examiné un échantillon de données de cyberdéfense, qui comprenait des communications privées interceptées par le CST en 2016–2017. En particulier, le bureau a examiné un échantillon correspondant à 36 pour cent des incidents cybernétiques et un certain nombre d'incidents choisis au hasard qui, selon ce qui a été indiqué, ne comportaient aucune communication privée. Au cours de la période visée par l'examen, le CST n'a pas intercepté de communications entre un conseiller juridique et son client. Comme

c'était le cas au cours des années passées, la majorité des communications privées interceptées consistaient en des courriels non sollicités envoyés par l'auteur d'une cybermenace à un employé du gouvernement du Canada.

INCIDENT CYBERNÉTIQUE

Acte malveillant ou événement suspect qui perturbe ou constitue une tentative de perturber le fonctionnement des dispositifs électroniques et des réseaux de communication importants pour le gouvernement du Canada. Un incident cybernétique peut comporter un ou plusieurs cyberévénements et une ou plusieurs communications privées.

Au cours de la période visée par l'examen, le commissaire a observé une hausse du nombre de communications privées utilisées ou conservées. L'année dernière, le CST a modernisé la base de données qui contient les données pour la cyberdéfense utilisées et conservées ainsi que le système de consignation des communications privées connexes que le CST recueille dans le cadre de son mandat en matière de sécurité des TI. Le CST a confirmé que la hausse du nombre de communications privées est principalement attribuable à cette modernisation, qui a amélioré la capacité du CST de découvrir et de conserver sans délai les renseignements pertinents sur les cybermenaces, notamment des communications privées. Les données interceptées, y compris les communications privées, peuvent être conservées ou utilisées par le CST seulement si l'interception était nécessaire pour identifier, isoler ou prévenir les activités dommageables visant les systèmes ou les réseaux informatiques du gouvernement du Canada. L'automatisation a permis d'uniformiser davantage les méthodes de dénombrement des communications privées du CST en ce sens que les communications privées sont automatiquement dénombrées au moment de leur conservation.

En examinant les communications privées au CST, le bureau du commissaire a remarqué l'existence de ce que le CST appelle des « communications privées recueillies de façon fortuite ». Il s'agit de communications privées qui **ne** sont **pas** essentielles à la protection des systèmes du gouvernement du Canada et qui sont enregistrées dans des dossiers pendant l'interception d'un réseau. Bien que le CST n'utilise pas ces communications privées recueillies de façon fortuite, il conserve les dossiers pendant 12 mois, car ceux-ci contiennent également des communications privées qui sont essentielles à la protection des systèmes du gouvernement du Canada. Les dossiers sont conservés pendant la période de validité de l'autorisation ministérielle, après quoi ils sont automatiquement détruits. Le bureau du commissaire accepte l'explication du CST selon laquelle il s'agit d'une limite technologique et a confirmé que la période de conservation est respectée pour la période d'examen en cours. Le commissaire continuera de

surveiller la façon dont le CST traite les communications privées recueillies de façon fortuite dans le cadre de ses examens annuels.

Pendant l'examen de l'échantillon, et guidé en partie par une activité trimestrielle de surveillance de la conformité du CST, le bureau du commissaire a relevé un dossier d'incident cybernétique réservé à un usage interne qui renfermait de l'information non supprimée sur l'identité d'un Canadien. Le document interne, que le CST utilise à des fins d'analyse de la cyberdéfense, est accessible à tous les analystes de cyberdéfense du CST. Même s'il était évident que l'information sur l'identité d'un Canadien contenue dans le dossier interne se rapportait à l'incident cybernétique, le bureau du commissaire s'est demandé s'il était nécessaire pour le CST d'inclure des renseignements personnels détaillés concernant la victime, plutôt que de simplement résumer les types de renseignements qui ont été découverts lors de l'incident cybernétique. Le bureau du commissaire a fait observer que même si des contrôles d'accès sont en place et que le dossier interne est accompagné d'une mise en garde au sujet de son utilisation et de sa conservation, à l'avenir, il serait possible de renforcer cette mise en garde en indiquant clairement qu'il faut assurer la protection de la vie privée lorsque le document comprend de l'information sur l'identité de Canadiens non supprimée. Le bureau du commissaire a encouragé le CST à tenir compte des répercussions que ses rapports et ses dossiers internes peuvent avoir sur la vie privée, et continuera de surveiller les cas où de l'information sur l'identité de Canadiens est incluse dans des dossiers internes.

Comme il a été souligné, la majorité des communications privées que le CST a dénombrées comme étant conservées ou utilisées en 2016–2017 consistaient en des courriels non sollicités envoyés par l'auteur d'une cybermenace à un employé du gouvernement du Canada. Ces courriels ne renfermaient rien de plus qu'un code malveillant ou un élément d'ingénierie sociale – c'est-à-dire qu'il n'y avait pas d'échange d'information personnelle ou d'autre information significative entre l'auteur de la cybermenace et l'employé. De façon contraire aux points de vue du commissaire, le CST dénombre ces types de communications comme étant des communications privées.

COMMUNICATIONS PRIVÉES DE CYBERDÉFENSE : CE QUE LE COMMISSAIRE DIT

« Une communication ne renfermant rien de plus qu'un code malveillant ou un élément d'ingénierie sociale envoyé à un système informatique de façon à lui porter atteinte n'est **pas** une communication privée au sens du *Code criminel*. »

Source : Rapport annuel 2015–2016 du commissaire du CST

Cependant, le CST a indiqué qu'il continuait de travailler avec le ministère de la Justice en vue de clarifier la définition d'une communication privée dans le contexte de la sécurité des TI, afin qu'elle soit conforme avec l'interprétation juridique de 2015–2016 du commissaire. Le bureau du commissaire a été informé que le CST envisage d'apporter un changement à sa procédure de dénombrement des communications privées de cyberdéfense, de façon à ce que celles qui sont générées par ordinateur (c.-à-d. les pourriels) soient éliminées du dénombrement officiel. Il est encourageant que le CST songe à revoir son interprétation de la définition d'une communication privée au sens du ***Code criminel***.

L'année dernière, le bureau du commissaire avait relevé un élargissement du nombre de situations où certaines informations sur l'identité de Canadiens associées à une infrastructure ciblée ou à laquelle il a été porté atteinte peuvent être divulguées, sans suppression, à des institutions du gouvernement du Canada, à des entités du secteur privé et à des alliés choisis. Le commissaire avait souligné que le CST devrait travailler avec ses alliés à mettre au point une entente sur le partage de renseignements aux fins de la cybersécurité. Le commissaire est heureux de confirmer que le CST a mis au point un énoncé de politique concernant le partage d'information sur l'identité en ce qui a trait aux activités de cyberdéfense avec ses alliés. La politique précise les types d'identité qui peuvent être diffusés, les conditions selon lesquelles ils peuvent être diffusés et les mises en garde qui doivent être respectées. Le commissaire a conclu que la politique est une référence acceptable pour le partage de telles informations, surtout compte tenu de la condition selon laquelle la diffusion doit être nécessaire à l'analyse et à l'atténuation de la menace à la cybersécurité.

Le commissaire s'était aussi engagé à faire un suivi du projet pilote du CST visant l'utilisation d'un système d'analyse des maliciels déployé au titre des pouvoirs existants du CST. Le bureau du commissaire a confirmé que la conservation des données et l'accès au système, qui est désormais opérationnel, sont conformes aux politiques actuelles du CST et font l'objet d'une surveillance trimestrielle de la conformité.

CONCLUSION

Le CST a pris des mesures pour donner suite à la recommandation formulée par le commissaire, au terme de l'examen de l'autorisation ministérielle de cyberdéfense de 2015–2016, selon laquelle le CST devrait diffuser des lignes directrices sur le marquage et le dénombrement uniformes de ce qui constitue des communications privées de cyberdéfense. Le CST a mis en œuvre de nouvelles lignes directrices et une nouvelle formation, et a modernisé la base de données qui contient les données pour la cyberdéfense utilisées et conservées, dans le but d'automatiser l'identification d'éventuelles communications privées et de normaliser le dénombrement des communications privées de cyberdéfense. Le

commissaire est heureux de confirmer que, grâce à ces mesures, le CST a suivi la recommandation.

Le CST n'a pas apporté de changements importants à la façon dont il mène ses activités de cyberdéfense ni aucun changement qui aurait présenté un risque pour la conformité à la loi ou la protection de la vie privée. Toutes les communications privées identifiées par le CST avaient été interceptées de façon non intentionnelle et traitées conformément aux politiques et aux procédures du CST – rien ne permettait de conclure que le CST aurait visé des Canadiens ou des personnes se trouvant au Canada au moyen de ses activités de cyberdéfense. Les communications privées utilisées et conservées par le CST étaient essentielles pour identifier, isoler ou prévenir les activités dommageables visant les systèmes ou les réseaux informatiques du gouvernement du Canada, conformément à la partie b) du mandat du CST en vertu de la *Loi sur la défense nationale*. Les communications privées qui n'étaient pas essentielles n'ont pas été conservées au-delà des périodes de conservation et de destruction prescrites par les politiques du CST.

Le commissaire continuera d'effectuer des examens annuels des autorisations ministérielles de cyberdéfense et des communications privées pour contrôler la conformité des activités en question ainsi que pour vérifier que le CST ne cible pas des Canadiens et qu'il protège la vie privée de ces derniers.

6. Examen combiné annuel des autorisations ministérielles du CST relatives à la collecte de renseignements électromagnétiques étrangers, 2016–2017 et 2017–2018 et vérification ponctuelle des « communications canadiennes »

CONTEXTE

Le présent résumé combine les constatations découlant de deux examens.

- **L'examen annuel des autorisations ministérielles du CST relatives à la collecte de renseignements électromagnétiques étrangers :** L'examen des autorisations ministérielles relatives à la collecte de renseignements électromagnétiques étrangers a été réalisé en vertu de la *Loi sur la défense nationale*, qui exige que le commissaire procède à l'examen des activités du CST exercées sous le régime d'autorisations ministérielles pour en contrôler la conformité et qu'il adresse au ministre un rapport annuel sur l'examen. Le bureau

a également examiné le statut, à la fin de la période de validité des autorisations ministérielles, des communications privées conservées ou utilisées par le CST qui avaient été interceptées sous le régime de ces autorisations ministérielles.

- **Une vérification ponctuelle de « communications canadiennes » :** La vérification ponctuelle a été effectuée dans le cadre du mandat principal du commissaire, lequel consiste à examiner les activités du CST pour s'assurer qu'elles sont conformes à la loi. La vérification portait sur des « communications canadiennes » conservées, utilisées ou détruites par le CST pendant une période de deux mois en 2017. Les communications comprennent celles qui ont été interceptées par des alliés et transmises au CST.

COMMUNICATIONS PRIVÉES ET « COMMUNICATIONS CANADIENNES »

On entend par **Canadien** un citoyen canadien, un résident permanent au sens du paragraphe 2(1) de la *Loi sur l'immigration et la protection des réfugiés* ou une personne morale constituée ou prorogée sous le régime d'une loi fédérale ou provinciale.

La **communication privée** est ainsi définie à l'article 183 du *Code criminel* : « communication orale ou télécommunication dont l'auteur se trouve au Canada, ou destinée par celui-ci à une personne qui s'y trouve, et qui est faite dans des circonstances telles que son auteur peut raisonnablement s'attendre à ce qu'elle ne soit pas interceptée par un tiers. La présente définition vise également la communication radiotéléphonique traitée électroniquement ou autrement en vue d'empêcher sa réception en clair par une personne autre que celle à laquelle son auteur la destine. »

Une « **communication canadienne** » désigne une communication entre deux interlocuteurs dont l'un se trouve physiquement au Canada (c'est-à-dire une communication privée) ou est un Canadien qui se trouve physiquement à l'extérieur du Canada. Une telle communication peut être acquise soit par le CST, soit par les partenaires de la Collectivité des cinq et transmise au CST.

Le CST mène des activités de collecte de renseignements électromagnétiques étrangers en vertu de l'alinéa 273.64(1)a) de la *Loi sur la défense nationale* – partie a) du mandat du CST – soit acquérir et utiliser l'information provenant de l'infrastructure mondiale d'information dans le but de fournir des renseignements étrangers, en conformité avec les priorités du gouvernement du Canada en matière de renseignement. Ces activités ne peuvent viser des Canadiens ou toute personne au Canada, et elles doivent être soumises à des mesures de protection

de la vie privée des Canadiens lors de l'utilisation et de la conservation des renseignements interceptés [alinéas 273.64(2)a) et b) de la *Loi sur la défense nationale*].

En vertu du paragraphe 273.65(1) de la *Loi sur la défense nationale*, le ministre peut, dans le seul but d'obtenir des renseignements étrangers, autoriser par écrit le CST à intercepter des communications privées liées à une activité ou une catégorie d'activités qu'il mentionne expressément. Comme les activités de collecte de renseignements électromagnétiques étrangers comportent un risque d'interception non intentionnelle de communications privées, le CST doit exercer ces activités sous le régime d'une autorisation ministérielle. Le CST peut conserver ou utiliser une communication privée interceptée uniquement si celle-ci est jugée essentielle aux affaires internationales, à la défense ou à la sécurité. Tous les renseignements recueillis qui sont utilisés dans un rapport sur les renseignements étrangers sont conservés pendant une période indéterminée par le CST.

INTERCEPTION FORTUITE OU NON INTENTIONNELLE?

Pour décrire l'interception d'une communication privée sous le régime d'une autorisation ministérielle, le CST emploie le mot « fortuit » (*incidental*) tandis que le bureau du commissaire emploie le terme « non intentionnel ». Pourquoi et quelle est la différence entre les deux qualificatifs?

Il y a interception « fortuite » d'une communication privée lorsque le CST intercepte une communication entre une entité étrangère située à l'extérieur du Canada et une personne au Canada.

Le terme « non intentionnel » constitue une description légale de l'interception « fortuite » d'une communication privée par le CST dans un contexte technique ou opérationnel. Ainsi, du point de vue légal, on peut dire de l'interception qu'elle était « non intentionnelle » puisqu'elle ne visait pas un Canadien ou une personne au Canada. Il s'agit plutôt d'un sous-produit ou d'un élément accessoire découlant du ciblage d'une entité étrangère située à l'extérieur du Canada.

Au cours de l'exercice 2017–2018, le CST a mené des activités de collecte de renseignements électromagnétiques étrangers sous le régime d'autorisations ministérielles, dont trois étaient en vigueur du 1er juillet 2016 au 30 juin 2017 et les trois autres du 1er juillet 2017 au 30 juin 2018. Le bureau s'est penché sur toutes ces autorisations ministérielles.

Les objectifs de l'examen étaient les suivants : veiller à ce que les activités aient été autorisées par le ministre, c'est-à-dire que les conditions d'autorisation énoncées au paragraphe 273.65(2) de la *Loi sur la défense nationale* ont été remplies; relever tout changement important – survenu dans les années visées par

l'examen comparativement aux années antérieures – aux documents d'autorisation ministérielle eux-mêmes ainsi qu'aux activités du CST ou à une catégorie d'activités décrites dans les autorisations ministérielles; et évaluer les répercussions des changements, le cas échéant, sur le risque de non-conformité à la loi ou le risque pour la vie privée.

Le bureau a examiné le statut, à la fin de la période de validité des autorisations ministérielles de 2016–2017, des communications privées identifiées que le CST avait acquises, conservées ou utilisées en exerçant ses activités de collecte de renseignements électromagnétiques étrangers. Le bureau a vérifié la conformité du CST à la loi et à toutes les autorisations, instructions ministérielles et politiques applicables, et a évalué la mesure dans laquelle le CST avait protégé la vie privée des Canadiens. En outre, le bureau du commissaire a fait une vérification ponctuelle, sans avoir donné de préavis au CST, de toutes les « communications canadiennes » (y compris des communications privées) utilisées ou conservées par le CST au cours d'une période de deux mois en 2017.

En ce qui concerne les communications privées acquises sous le régime d'une autorisation ministérielle et les « communications canadiennes » visées par la vérification ponctuelle, le bureau a examiné tous les rapports sur les renseignements étrangers établis par le CST qui se fondaient en totalité ou en partie sur ces communications. Le bureau a également reçu des comptes rendus sur l'ensemble des communications conservées, il a vu de ses propres yeux un échantillon de ces communications et il a interviewé les analystes du renseignement étranger et les superviseurs concernés qui mettaient en œuvre les priorités du gouvernement en matière de renseignement au sujet des motifs sur lesquels ils s'appuyaient pour conserver les communications.

CONSTATATIONS ET RECOMMENDATIONS

Le commissaire a constaté que les autorisations ministérielles de 2016–2017 et de 2017–2018 relatives à la collecte de renseignements électromagnétiques étrangers remplissaient les conditions d'autorisation définies dans la ***Loi sur la défense nationale***, à savoir :

- l'interception visait des entités étrangères situées à l'extérieur du Canada;
- les renseignements à obtenir ne pouvaient raisonnablement être obtenus d'une autre manière;
- la valeur des renseignements étrangers que l'on espérait obtenir grâce à l'interception justifiait l'interception envisagée; et
- il existait des mesures satisfaisantes pour protéger la vie privée des Canadiens et pour faire en sorte que les communications privées ne soient utilisées ou conservées que si elles étaient essentielles aux affaires internationales, à la défense ou à la sécurité.

Il n'y avait aucun changement important dans les autorisations ministérielles de 2016-2017 et de 2017-2018 ni dans les mémoires de demande connexes adressés au ministre. Toutefois, il a été établi que le mémoire de demande lié à l'une des autorisations ministérielles était moins détaillé que par les années passées. En 2017-2018, le CST a révisé le mémoire de demande se rapportant à l'une des autorisations ministérielles afin de décrire de façon uniforme les activités d'échantillonnage et de sélection du CST. Bien que la quête d'uniformité soit encourageante, le commissaire a conclu que les efforts déployés en ce sens avaient entraîné la perte de certains renseignements concernant le processus et l'explication technique, ce qui fait que le mémoire ne fournit peut-être pas le plus d'information possible aux fins de la prise d'une décision par le ministre. Par conséquent, le commissaire **a recommandé** que le CST veille à ce que les mémoires de demande ultérieurs liés aux autorisations ministérielles contiennent de l'information détaillée de façon à décrire et à expliquer de manière exhaustive les activités de collecte de renseignements électromagnétiques étrangers envisagées par le CST, afin de mieux aider le ministre à prendre une décision.

PROTECTION DE LA VIE PRIVÉE DES CANADIENS

Le CST se voit interdire, dans le cadre de ses activités de collecte de renseignements électromagnétiques étrangers et de cyberdéfense, de cibler des Canadiens – où qu'ils se trouvent dans le monde – ou toute personne au Canada. Le fait que le travail du CST vise des cibles étrangères signifie que, à la différence des autres organismes de renseignement et de sécurité du Canada, le CST a des interactions limitées avec les Canadiens. Lorsque le CST acquiert fortuitement de l'information se rapportant à un Canadien, il est tenu par la loi de prendre des mesures pour protéger la vie privée de ce Canadien. Dans le cadre de son examen des activités du CST, le commissaire vérifie entre autres si le CST ne cible pas des Canadiens et s'il applique efficacement des mesures satisfaisantes pour protéger la vie privée des Canadiens dans toutes les activités opérationnelles qu'il entreprend.

En 2016-2017, le nombre de communications privées identifiées qui ont été interceptées de façon non intentionnelle a continué d'augmenter considérablement. La hausse du nombre de communications privées identifiées demeure une conséquence des caractéristiques techniques de technologies de communication particulières et de l'obligation légale du CST de dénombrer les communications privées d'une certaine façon. Malgré la hausse du nombre de communications privées interceptées, le nombre de communications privées qui ont été utilisées ou conservées a diminué d'environ 70 pour cent, passant de 3 348 à 954, à la fin de la période de validité de l'autorisation ministérielle de 2016-2017.

De ces 954 communications privées, le CST a utilisé 261 communications privées dans 14 rapports sur les renseignements étrangers et a par la suite détruit les communications privées restantes.

Pendant la vérification ponctuelle, le bureau a également examiné toutes les « communications canadiennes » qui avaient été non intentionnellement acquises par le CST lors de la période visée par la vérification, et identifiées comme telles par la suite. Cela incluait tant des communications marquées pour conservation que des communications marquées pour destruction par le CST comme étant non essentielles aux affaires internationales, à la défense ou à la sécurité.

Le bureau a confirmé que les « communications canadiennes » jugées non essentielles ont été détruites.

À la lumière de l'information examinée et des entretiens menés, le commissaire a conclu que le CST avait agi en conformité avec la loi et qu'il avait protégé la vie privée des Canadiens. En particulier :

- les activités relatives à la collecte de renseignements électromagnétiques étrangers du CST ne visaient pas des Canadiens ou des personnes se trouvant au Canada;
- les « communications canadiennes » identifiées par le CST avaient été interceptées de façon non intentionnelle;
- les « communications canadiennes » utilisées et conservées par le CST étaient essentielles aux affaires internationales, à la défense ou à la sécurité, comme l'exige la ***Loi sur la défense nationale***;
- le CST avait détruit les « communications canadiennes » non essentielles; et
- le CST avait exercé ses activités relatives à la collecte des renseignements électromagnétiques étrangers conformément aux directives et aux autorisations ministérielles et avait traité les « communications canadiennes » conformément à ses politiques et à ses procédures – le CST n'avait pas conservé de communications privées au-delà des périodes de conservation et de destruction prescrites par ses politiques.

Définition des communications entre un conseiller juridique et son client

Le bureau du commissaire a relevé un changement dans la terminologie utilisée par le CST dans les trois autorisations ministérielles concernant les communications entre un conseiller juridique et son client. Les autorisations précisent les mesures à prendre quand un analyste du CST identifie une communication entre un client et un « conseiller juridique canadien ». Le bureau du commissaire a demandé une explication au CST relativement à l'ajout du qualificatif « canadien », lequel ne figurait pas explicitement dans les autorisations ministérielles

antérieures. Le CST a répondu que le qualificatif « canadien » n'était pas nouveau et qu'il avait été intégré aux autorisations ministérielles dans un souci de clarté. Le commissaire est d'avis que l'intégration de ce qualificatif crée une ambiguïté.

Le terme « canadien » évoque la citoyenneté, indépendamment du lieu où se trouve le conseiller juridique. Au sens de la ***Loi sur la défense nationale***, le terme « Canadien » s'entend d'un citoyen canadien, d'un résident permanent ou d'une personne morale constituée au Canada. Le commissaire s'attend à ce que les termes employés dans les autorisations ministérielles soient conformes aux définitions prévues par la ***Loi sur la défense nationale***. Dans la pratique, cependant, le CST se fonde sur la définition d'une communication entre un conseiller juridique et son client qui se trouve dans sa politique générale sur la protection de la vie privée, laquelle ne comprend pas le terme « canadien » et ne fait pas mention de la citoyenneté ni du lieu géographique. La définition repose plutôt sur la question de savoir si la personne est autorisée à pratiquer le droit au Canada.

Le problème touche à la fois les autorisations ministérielles relatives à la collecte de renseignements électromagnétiques étrangers et celles qui se rapportent à la sécurité des technologies de l'information. Par conséquent, **le commissaire a fait la même recommandation** que celle qu'il a formulée lors de son examen annuel des activités de cyberdéfense du CST menées sous le régime de l'autorisation ministérielle en vigueur en 2016–2017, c'est-à-dire que le CST clarifie la terminologie employée dans ses autorisations ministérielles pour veiller à ce qu'elle reflète fidèlement la protection juridique reconnue et offerte relativement aux communications entre un conseiller juridique et son client dans le droit canadien, et pour assurer l'uniformité avec la terminologie utilisée dans ses politiques et pratiques relatives aux activités en matière de sécurité des technologies de l'information et aux activités de collecte de renseignements électromagnétiques étrangers.

Contexte juridique en évolution

Récemment, la Cour suprême du Canada s'est penchée sur deux affaires (*R. c. Marakah*, 2017 CSC 59 et *R. c. Jones*, 2017 CSC 60) qui portaient sur les notions d'« interception » et de « fouille » dans le contexte des technologies en évolution. Ces affaires présentaient un intérêt puisqu'elles auraient pu avoir une incidence sur le traitement des « communications canadiennes » acquises dans le cadre d'un des programmes de collecte de renseignements électromagnétiques étrangers du CST. En fin de compte, les décisions rendues n'ont pas eu de répercussions sur les activités du CST; toutefois, le contexte juridique en évolution pourrait influer sur les lignes directrices relatives à la façon dont certaines « communications canadiennes » seront traitées à l'avenir. Le commissaire surveillera tout élément nouveau sur le plan juridique et son incidence sur les activités du CST.

CONCLUSION

Depuis le dernier examen des autorisations ministérielles relatives aux activités de collecte de renseignements électromagnétiques étrangers, le CST a donné suite à deux recommandations formulées dans le rapport annuel de l'année dernière : une des recommandations avait été formulée lors de l'examen de l'autorisation ministérielle relative à la collecte de renseignements électromagnétiques étrangers, et l'autre dans le cadre de la vérification ponctuelle. La première recommandation proposait qu'en raison des caractéristiques techniques de certaines technologies de communication, les rapports du CST au ministre sur les communications privées devraient renfermer des renseignements supplémentaires pour mieux décrire ces communications et expliquer l'ampleur de l'atteinte à la vie privée; la façon dont le CST dénombre actuellement les communications privées donne une vision déformée du nombre de Canadiens ou de personnes au Canada qui sont interlocuteurs dans une communication interceptée par le CST afin d'obtenir des renseignements étrangers sous le régime d'une autorisation ministérielle. Dans son rapport de fin d'exercice présenté au ministre sur les autorisations ministérielles de 2016–2017, le CST a fourni des renseignements supplémentaires au ministre pour expliquer la raison de la hausse considérable du nombre de communications privées identifiées. Le commissaire s'est dit satisfait de cela.

La deuxième recommandation proposait que chaque fois qu'il envisage d'utiliser ou de conserver une communication interceptée qui est protégée par le secret professionnel de l'avocat, le CST devrait toujours obtenir un avis juridique écrit auprès du ministère de la Justice concernant le caractère privilégié de la communication et concernant la question de savoir si son utilisation ou sa conservation est conforme aux lois canadiennes. Le CST a modifié sa politique pour décrire ce que les employés du CST doivent faire lorsqu'ils traitent des communications entre un conseiller juridique et son client qui ont été recueillies dans le cadre du mandat du CST en matière de collecte de renseignements électromagnétiques étrangers, y compris obtenir un avis juridique et conserver les dossiers qui rendent compte des décisions prises et des avis juridiques obtenus.

Le bureau du commissaire continuera d'effectuer des examens annuels des autorisations ministérielles liées à la collecte des renseignements électromagnétiques étrangers, ainsi que des examens des activités de collecte de renseignements électromagnétiques étrangers exercées par le CST sous le régime des autorisations ministérielles. Le bureau procédera également à des vérifications ponctuelles approfondies des « communications canadiennes » acquises et identifiées par le CST, qu'elles aient été recueillies par le CST ou par un allié. En outre, le bureau du commissaire a l'intention d'examiner, dans le cadre d'un examen de suivi, la façon dont les différents programmes du CST peuvent se compléter et l'incidence qu'ils peuvent avoir les uns sur les autres.

Enfin, le commissaire surveillera les mesures prises par le CST pour régler les questions relevées dans le présent rapport.

7. Examen annuel des Dossiers relatifs aux incidents liés à la vie privée et du Dossier des erreurs de procédure mineures

CONTEXTE

Le CST signale et documente tout incident associé à ses activités opérationnelles ou à celles de ses alliés où il pourrait y avoir eu atteinte à la vie privée d'un Canadien, contrairement aux politiques ou aux procédures opérationnelles du CST en matière de protection de la vie privée des Canadiens ou de toute personne au Canada.

Ces incidents, ainsi que les mesures correctives prises, sont consignés dans un des trois dossiers en fonction de l'endroit où l'incident est survenu et de son potentiel de causer un dommage. Il s'agit du Dossier relatif aux incidents liés à la vie privée (DIVP), du Dossier relatif aux incidents liés aux alliés (DIA) et du Dossier des erreurs de procédure mineures (DEPM) tenus par le CST.

Le DIVP est un dossier des incidents attribuables au CST concernant de l'information sur un Canadien ou toute personne au Canada qui a été traitée de manière contraire à la politique de protection de la vie privée du CST et qui a été exposée à des parties externes ne devant pas l'avoir reçue. Ce type de manipulation inadéquate est désigné « incident lié à la vie privée ». Le DIA est un dossier des incidents liés à la vie privée qui sont attribuables à des alliés. Ces incidents peuvent être signalés par les alliés mêmes ou par le CST. Enfin, le DEPM est un dossier des cas où le CST a traité de manière inappropriée de l'information sur un Canadien, mais où l'information a été contenue au sein du CST et n'a pas été exposée à des parties externes.

L'examen annuel par le bureau du DIVP, du DIA et du DEPM met l'accent sur les incidents qui n'ont pas été examinés en détail dans le cadre d'autres examens. L'examen offre une occasion de déterminer les tendances ou les faiblesses systémiques qui pourraient indiquer que des mesures correctives, des changements aux procédures ou aux politiques du CST ou un examen approfondi d'une activité ou d'un incident précis s'imposent. Par exemple, le bureau pourrait exercer une fonction d'examen critique afin de déterminer si l'un des incidents survenus dans le cadre des opérations constituait une « atteinte substantielle à la vie privée », ce que la politique pangouvernementale définit comme une atteinte visant des renseignements personnels sensibles dont on peut raisonnablement penser qu'elle risque de causer un préjudice ou un dommage sérieux à la personne, ou touche un nombre élevé de personnes.

En plus d'examiner les erreurs de procédure, les incidents et les mesures subséquentes prises par le CST pour corriger la situation ou atténuer les répercussions, l'examen avait les objectifs suivants : établir si des incidents survenus dans

le cadre des opérations constituaient des atteintes substantielles à la vie privée; déterminer si tout incident soulève des questions de conformité à la loi ou de protection de la vie privée des Canadiens; et évaluer le cadre de validation de la conformité à la politique du CST et les activités de surveillance dans ce contexte. La période visée par l'examen allait du 1er juillet 2016 au 30 juin 2017.

Le bureau a examiné les 81 incidents liés à la vie privée consignés dans le DIVP (48) et le DIA (33), ainsi que les mesures correctives prises par le CST pour y remédier. Le bureau a également examiné les dix erreurs de procédure mineures documentées par le CST au cours de la période visée.

CONSTATATIONS

La plupart des incidents liés à la vie privée consignés dans le DIVP et le DIA se rapportaient au partage d'information sur l'identité de Canadiens ou à son intégration par inadvertance à un rapport sans la supprimer, comme l'exige la politique du CST, ainsi qu'au ciblage non intentionnel ou à des recherches dans les bases de données visant des renseignements sur des personnes jusqu'alors non connues pour être des Canadiens ou des personnes au Canada. Dans tous les cas, les rapports ont été annulés ou corrigés et l'information sur l'identité a été dûment supprimée, ou le CST a radié toute communication interceptée ou tout rapport connexe.

INFORMATION SUR L'IDENTITÉ DE CANADIENS

L'information sur l'identité de Canadiens est celle pouvant être utilisée pour identifier un Canadien ou une organisation ou une société canadienne dans le contexte de renseignements personnels ou commerciaux. L'information sur l'identité de Canadiens comprend, sans s'y limiter, les noms, les numéros de téléphone, les adresses de courriel, les adresses de protocole Internet et les numéros de passeport. Lorsque le CST intègre de l'information sur l'identité de Canadiens à un rapport, il doit la supprimer et la remplacer par une mention générique, telle que « Canadien nommé », afin de protéger l'identité de ce Canadien.

Deux incidents étaient liés à un manque de connaissance ou de compréhension de la part de groupes n'appartenant pas au CST en ce qui concerne les politiques du CST sur la protection de la vie privée des Canadiens : un groupe appartenait à un allié et l'autre à un partenaire canadien. Dans les deux cas, le groupe concerné a reçu de son organisation des documents de sensibilisation aux politiques visant à corriger les lacunes.

Pour une troisième année consécutive, le DIVP comprenait un incident lié à un rapport d'un partenaire de la Collectivité des cinq renfermant de l'information sur un Canadien ou une personne au Canada qui a été transmis au Service canadien du renseignement de sécurité par l'entremise du CST et qui aurait dû faire l'objet d'une diffusion interne restreinte, mais qui a été partagé au sein du CST. Cependant, le rapport a été distribué dans une situation d'urgence où il y avait un danger pour la vie. Le commissaire était convaincu que, même si les mesures prises par l'employé allaient à l'encontre de la politique du CST, la réponse du CST était appropriée dans les circonstances. Le bureau a plus tard été informé que des mesures stratégiques correctives ont été officialisées. L'incident sera examiné de façon approfondie dans le cadre de l'examen, par le bureau, de l'assistance fournie par le CST au Service canadien du renseignement de sécurité concernant ce type d'activité, qui débutera au cours du prochain exercice.

Un incident consigné dans le DIVP se rapportait à un outil de collecte défectueux qui a permis à de l'information sur l'identité de Canadiens d'être transférée dans les bases de données du CST pendant une dizaine de jours. L'outil a été réparé, et les données qui avaient été recueillies par inadvertance ont été purgées des systèmes du CST.

Le commissaire a convenu avec le CST que toutes les erreurs consignées dans le DEPM étaient des erreurs mineures ne constituant pas des incidents liés à la vie privée. Ces erreurs de procédure comprenaient, par exemple : des fichiers non ouverts qui auraient pu contenir de l'information sur l'identité de Canadiens qui ont été conservés au-delà de la période de conservation autorisée; une liste servant à contrôler l'accès à certains types d'information qui a connu une défaillance technique et qui, de façon temporaire, n'a pas désactivé l'accès de personnes dont les justificatifs d'identité n'étaient plus valides; de l'information sur l'identité de Canadiens qui a été temporairement visible dans un outil de communication interne; et un autre système de collecte défectueux qui, pendant un certain temps, risquait de recueillir des communications où les deux interlocuteurs sont canadiens ou se trouvent au Canada, mais ne l'a pas fait. Ces incidents sont considérés avoir un effet moindre sur la vie privée puisqu'ils restent à l'interne et qu'ils sont réglés avant que quelqu'un à l'extérieur du CST ne consulte l'information.

Après examen des trois dossiers, des réponses obtenues du CST, ainsi que des dossiers connexes du CST, le commissaire a conclu que, dans tous les cas, le CST a pris les mesures correctives appropriées, y compris, le cas échéant, des mesures pour prévenir des occurrences similaires à l'avenir.

Selon la politique pangouvernementale, il incombe au ministère ou à l'organisme de signaler les atteintes substantielles à la vie privée. Le CST n'a pas signalé d'atteinte substantielle à la vie privée dans le cadre de ses opérations pour la période visée. Le commissaire a convenu que les incidents énumérés dans le

DIVP et le DIA pour la période visée ne constituaient pas des atteintes substantielles à la vie privée.

CONCLUSION

Cet examen n'a pas mis au jour des atteintes substantielles à la vie privée, des lacunes systémiques ou des questions nécessitant un examen de suivi qui n'était pas déjà prévu. Le CST a signalé qu'il n'était au courant d'aucune incidence négative sur les Canadiens concernés par un des incidents liés à la vie privée.

Le commissaire était convaincu que le CST a réagi comme il se doit aux incidents liés à la vie privée et aux erreurs de procédure mineures relevés durant la période visée.

L'enregistrement et le signalement des incidents liés à la vie privée et des erreurs de procédure mineures demeurent un moyen efficace pour le CST de promouvoir le respect des obligations légales, des exigences ministérielles et des politiques et procédures opérationnelles, et d'améliorer la protection de la vie privée des Canadiens. Les améliorations apportées aux rapports et aux structures de dossiers connexes devraient permettre de renforcer les mesures de protection de la vie privée.

Le commissaire n'a formulé aucune recommandation. Toutefois, il a encouragé le CST à assurer l'uniformité quant au sens des termes utilisés lorsqu'il rend compte de ses activités de collecte de renseignements électromagnétiques étrangers et de ses activités en matière de sécurité des technologies de l'information.

PLAINTES CONCERNANT LES ACTIVITÉS DU CST

En 2017-2018, le bureau a été contacté par plusieurs personnes en quête d'information ou exprimant des préoccupations concernant les activités du CST. Toutefois, il a été déterminé que les demandes de renseignements ne relevaient pas du mandat du commissaire, ne se rapportaient pas aux activités opérationnelles du CST ou manquaient de sérieux. Aucune plainte concernant les activités du CST ne justifiait une enquête.

MANDAT SOUS LE RÉGIME DE LA *LOI SUR LA PROTECTION DE L'INFORMATION*

Le commissaire est tenu en vertu de la *Loi sur la protection de l'information* de recevoir de l'information émanant de personnes astreintes au secret à perpétuité qui ont l'intention de communiquer des renseignements opérationnels spéciaux – par exemple certains renseignements se rapportant aux activités du CST en faisant valoir la primauté de l'intérêt public. Aucune affaire de ce genre n'a été signalée au commissaire en 2017-2018.

ACTIVITÉS DU BUREAU DU COMMISSAIRE

MODIFICATIONS LÉGISLATIVES

Tout au long de l'année, le commissaire et ses fonctionnaires ont consacré des efforts considérables à l'examen de deux projets de loi déposés devant le Parlement qui visent à renforcer la reddition de comptes des ministères et organismes fédéraux qui exercent des activités relatives à la sécurité nationale.

Les deux projets de loi proposaient des changements importants en ce qui a trait au contexte du renseignement et de la sécurité au Canada. Le commissaire Plouffe a rencontré les ministres de la Défense nationale et de la Sécurité publique, le conseiller à la sécurité nationale et au renseignement auprès du premier ministre, et la chef du CST. Le personnel du commissaire a tenu de nombreuses réunions avec des représentants du CST, du Service canadien du renseignement de sécurité (SCRS), de Sécurité publique Canada, du Bureau du Conseil privé et du Comité de surveillance des activités de renseignement de sécurité (CSARS). Les échanges,

qui se sont révélés fructueux, ont permis d'enrichir la compréhension de tous les participants et de favoriser une analyse plus poussée des idées présentées dans les projets de loi.

PROJET DE LOI C-22

Dans la foulée de la restructuration du cadre de reddition de comptes en matière de sécurité nationale, le projet de loi C-22, ***Loi constituant le Comité des parlementaires sur la sécurité nationale et le renseignement*** (CPSNR), a été déposé à la Chambre des communes en 2016. Lors de sa comparution devant le Comité sénatorial permanent de la sécurité nationale et de la défense le 12 juin 2017, le commissaire Plouffe a exposé sa vision concernant l'établissement d'une relation de travail productive avec le CPSNR pour aider à faire en sorte que l'utilisation des ressources de chacun soit efficace et efficiente. Il a aussi souligné des facteurs à prendre en considération pour éviter le chevauchement des efforts entre le CPSNR et les organismes d'examen.

Le projet de loi a reçu la sanction royale le 22 juin 2017; les membres du comité ont été nommés à l'automne 2017 et le directeur exécutif du secrétariat du CPSNR a été nommé en janvier 2018.

PROJET DE LOI C-59

Au cours de la même semaine pendant laquelle le projet de loi C-22 a été adopté, le gouvernement a déposé un autre projet de loi important, soit le projet de loi C-59, ***Loi concernant des questions de sécurité nationale***. Le projet de loi a été envoyé au Comité permanent de la sécurité publique et nationale (SECU) de la Chambre des communes avant la deuxième lecture, plutôt que d'être envoyé après la deuxième lecture conformément à la pratique habituelle. Comme l'a dit le ministre Goodale, le gouvernement a choisi de procéder ainsi pour permettre d'accueillir la présentation de nouvelles idées et d'autres suggestions avant la deuxième lecture.

Le projet de loi, qui compte dix parties, est complexe et vise à transférer la fonction d'examen du bureau à l'Office (proposé) de surveillance des activités en matière de sécurité nationale et de renseignement. Il prévoit aussi que le commissaire du CST deviendra le commissaire au renseignement, qui participera au processus décisionnel concernant certaines activités proposées par le CST et le SCRS avant que les activités puissent être entreprises.

Le 30 janvier 2018, le commissaire Plouffe a comparu devant le SECU en compagnie du directeur exécutif et du conseiller juridique spécial du bureau. Le commissaire a fait ressortir plusieurs des propositions qu'il avait formulées dans la présentation écrite au SECU, y compris des suggestions visant à élargir le rôle

du commissaire au renseignement de façon à ce qu'il corresponde aux nouveaux pouvoirs du CST.

À la fin de l'année, le CST et le ministère de la Justice ont organisé des séances d'information pour aider les autres ministères et organismes qui mènent des activités liées à la sécurité nationale à mieux comprendre les répercussions du projet de loi C-59 sur leurs opérations. Le bureau du commissaire était heureux de participer aux séances et d'expliquer les aspects visés et non visés par un examen ainsi que la manière dont un examen est effectué. Le fait de préparer ces ministères et organismes à la façon dont ils pourraient être touchés contribue à faire en sorte que les attentes soient réalistes de même qu'à dissiper les préoccupations.

SENSIBILISATION, APPRENTISSAGE ET RÉSEAUTAGE

Le commissaire et son bureau représentent l'intérêt public en ce qui a trait à la reddition de comptes du CST, car le CST doit en grande partie exercer ses activités en secret. Les activités de sensibilisation, de réseautage et d'apprentissage du bureau contribuent à la transparence dont le commissaire s'efforce de faire preuve et renforcent la capacité du bureau d'exécuter le mandat du commissaire.

En août, le directeur exécutif a présenté un exposé dans le cadre d'un cours d'été destiné à des étudiants de cycle supérieur à l'Université d'Ottawa. Il a parlé du passé et de l'avenir de la fonction d'examen, décrivant le rôle actuel du commissaire et en quoi le projet de loi C-59 pourrait restructurer le cadre de reddition de comptes en matière de sécurité nationale.

En octobre, l'Association des communications et de l'électronique des Forces canadiennes a organisé un symposium des cyberopérations à Kingston, en Ontario, qui a réuni des intervenants du gouvernement et de l'industrie ainsi que des spécialistes du milieu universitaire. Le directeur exécutif a participé à une réunion d'experts portant sur le projet de loi relatif à la surveillance des activités liées à la sécurité nationale et ses répercussions sur les cyberopérations.

En mars, deux conseillers juridiques du bureau du commissaire se sont adressés à des étudiants de cycle supérieur de l'Université de Sherbrooke pour leur expliquer les pouvoirs et les activités du commissaire. Ils étaient accompagnés de représentants du CSARS et du secrétariat du CPSNR.

En février 2018, le directeur exécutif a assisté à la 19e conférence annuelle sur la sécurité et la protection de la vie privée qui s'est tenue à Victoria, en Colombie-Britannique. Cet événement important, à l'occasion duquel le directeur exécutif a déjà pris la parole à deux reprises, réunit des représentants du gouvernement, de l'industrie et du milieu universitaire pour discuter des nouveautés au Canada et à l'échelle internationale en ce qui a trait à la technologie, à la sécurité et à la protection de la vie privée.

Tout au long de l'année, le personnel du bureau a assisté à des conférences portant sur les affaires internationales, la sécurité des technologies de l'information, la sécurité nationale, la protection de la vie privée et la cybersécurité. Il s'agissait de conférences tenues par des organisations telles que le Réseau intégré sur la cybersécurité, l'Association canadienne pour les études de renseignement et de sécurité et divers établissements universitaires.

Grâce à la formation, le personnel du bureau a veillé au respect et au renforcement des normes professionnelles dans divers domaines, dont le droit, l'accès à l'information et la protection de la vie privée ainsi que la sécurité des communications.

En outre, un atelier d'une journée et demie portant sur l'examen – une initiative que le bureau du commissaire a lancée il y a huit ans – a été organisé en février. Conçu pour combler une lacune en matière de formation pour les examinateurs des organismes de renseignement et de sécurité, en particulier le personnel qui débute dans le domaine de l'examen, le dernier atelier a été présenté aux employés de la Commission civile d'examen et de traitement des plaintes relatives à la Gendarmerie royale du Canada, du CSARS et du secrétariat du CPSNR, en plus des employés du bureau du commissaire.

Le bureau a aussi continué de présenter des exposés sur son travail aux nouveaux employés du CST dans le cadre du programme d'apprentissage fondamental de celui-ci. Plusieurs employés du bureau ont suivi des cours au CST, ce qui leur a permis de recevoir la même information que celle transmise aux employés du CST.

RÉUNIONS AVEC D'AUTRES ORGANISMES D'EXAMEN

L'an dernier, le commissaire a présenté un compte rendu des réunions que lui et son collègue, le président du CSARS, avaient eues à Washington, D.C. en 2016 avec leurs homologues des États-Unis, du Royaume-Uni, de l'Australie et de la Nouvelle-Zélande. De telles réunions sont essentielles dans un contexte où des modifications législatives importantes ont des répercussions sur les structures de reddition de comptes et créent de nouveaux pouvoirs pour les organismes de sécurité et de renseignement dans nos pays respectifs.

La réunion de Washington a abouti à une entente visant à établir le Five Eyes Intelligence Oversight and Review Council (conseil de surveillance et d'examen des activités de renseignement de la Collectivité des cinq). La première réunion en personne de ce conseil s'est déroulée sur deux jours, en octobre, et a été organisée conjointement par le commissaire du CST et le président du CSARS. Tous les participants ont convenu que les discussions avaient été très constructives et qu'elles aideront à renforcer la reddition de comptes générale concernant les activités liées à la sécurité et au renseignement dans leurs pays respectifs. Le conseil a établi qu'une réunion en personne aura lieu chaque année, et que des vidéoconférences seront organisées entre les réunions annuelles.

L'un des facteurs ayant motivé la création du conseil est l'abandon de la Conférence internationale des organismes de surveillance du renseignement. Bien que le conseil permette au commissaire d'établir des liens plus étroits avec ses homologues de la Collectivité des cinq, le commissaire s'efforce également de demeurer en contact avec un certain nombre de ses autres homologues internationaux qui avaient participé à la conférence.

D'autres réunions ont eu lieu au Canada avec des fonctionnaires étrangers, notamment avec le commissaire aux pouvoirs d'enquête du Royaume-Uni en octobre et avec le coordonnateur national de la sécurité et du contre-terrorisme des Pays-Bas en mars. En novembre, le bureau a aussi participé à une réunion axée sur la surveillance du renseignement avec le comité parlementaire de la sécurité de la République italienne (Parliamentary Committee for the Security of the Italian Republic), qui avait été organisée par le CSARS.

PLAN DE TRAVAIL – EXAMENS EN COURS ET PRÉVUS

Le commissaire adopte une approche préventive axée sur le risque pour réaliser ses examens, établissant les priorités en matière d'examen en se concentrant sur les domaines où les risques de non-conformité à la loi sont évalués comme étant les plus élevés ou comme étant une menace possible pour la vie privée des Canadiens. Un plan de travail triennal est mis à jour deux fois par an. L'élaboration du plan de travail repose sur maintes sources, notamment les séances d'information régulières du CST sur les nouvelles activités et les changements touchant les activités existantes, le rapport annuel classifié présenté par le chef du CST au ministre et faisant état des priorités du CST et des questions importantes sur le plan juridique, politique, opérationnel ou en matière de gestion, et les problèmes relevés dans les examens passés ou en cours. Pour apprendre davantage sur l'approche préventive axée sur le risque adoptée par le commissaire pour effectuer ses examens, veuillez consulter le site Web du bureau.

Une fois le projet de loi C-59 en vigueur, les examens en cours du bureau du commissaire seront transférés à l'Office de surveillance des activités en matière de sécurité nationale et de renseignement en vue d'être achevés. Toutefois, le bureau s'attend à ce que les quatre examens qui ont été amorcés en 2017–2018 seront achevés en 2018–2019. Il s'agit des examens suivants : un examen portant sur une méthode particulière de collecte de renseignements électromagnétiques étrangers menée sous le régime d'une autorisation ministérielle et d'une directive ministérielle; un examen des activités de ciblage du CST; un examen de l'assistance fournie par le CST au Service canadien du renseignement de sécurité (SCRS) en vertu de la partie c) du mandat du CST ainsi que des articles 12 et 21 de la ***Loi sur le SCRS*** (auparavant, ce type d'assistance du CST était fourni sous le régime de ce qu'on appelait les « mandats d'interception au Canada de télécommunications étrangères »); et un examen distinct qui fait suite à l'examen achevé en 2016–2017 sur les divulgations par le CST d'information sur l'identité de Canadiens.

Un examen de suivi sera également mené, qui portera sur le soutien apporté par le CST au SCRS en vertu de la partie c) de son mandat concernant un certain type de rapport mettant en cause des Canadiens.

En outre, le commissaire continuera d'effectuer des examens annuels portant sur :

- les autorisations ministérielles de collecte de renseignements électromagnétiques étrangers et de cyberdéfense, y compris les vérifications ponctuelles de « communications canadiennes » acquises et identifiées par le CST;
- les divulgations par le CST d'information sur l'identité de Canadiens; et
- les incidents liés à la vie privée et les erreurs de procédure mises au jour par le CST ainsi que les mesures qu'il a prises par la suite pour y remédier.

ANNEXE A : BIOGRAPHIE DE L'HONORABLE JEAN-PIERRE PLOUFFE, CD

L'honorable Jean-Pierre Plouffe a été nommé commissaire du Centre de la sécurité des télécommunications le 18 octobre 2013 pour un mandat de trois ans. Le 18 octobre 2016, son mandat a été renouvelé pour une période de deux ans.

Né le 15 janvier 1943 à Ottawa, en Ontario, M. Plouffe a fait ses études à l'Université d'Ottawa où il a obtenu sa licence en droit ainsi qu'une maîtrise en droit public (droit constitutionnel et international). Il a été admis au barreau du Québec en 1967.

M. Plouffe a débuté sa carrière au cabinet du juge-avocat général des Forces armées canadiennes. Il a pris sa retraite de la Force régulière en 1976, alors qu'il était lieutenant-colonel, mais est demeuré dans la Force réserve jusqu'en 1996. Il a été avocat en pratique privée au sein du cabinet Séguin, Ouellette, Plouffe et associés, à Gatineau, au Québec, où il s'est spécialisé en droit criminel, a agi en tant que président du tribunal disciplinaire des pénitenciers fédéraux, ainsi qu'en tant qu'avocat de la défense en cour martiale. Par la suite, M. Plouffe a travaillé pour le bureau d'aide juridique en qualité de directeur de la section de droit criminel.

M. Plouffe a été nommé juge militaire en 1980 (Force de réserve), puis juge à la Cour du Québec en 1982. Pendant plusieurs années, il a été chargé de cours en procédure pénale à la Section de droit civil de l'Université d'Ottawa. Il a ensuite été nommé juge à la Cour supérieure du Québec en 1990, puis juge à la Cour d'appel de la cour martiale du Canada en mars 2013. Il a pris sa retraite en tant que juge surnuméraire le 2 avril 2014.

Au cours de sa carrière, M. Plouffe a participé à la fois à des activités professionnelles et communautaires. Il a reçu des distinctions honorifiques civiles et militaires.

ANNEXE B : EXTRAITS DE LA *LOI SUR LA DÉFENSE NATIONALE* ET DE LA *LOI SUR LA PROTECTION DE L'INFORMATION* RELATIFS AU MANDAT DU COMMISSAIRE

LOI SUR LA DÉFENSE NATIONALE – PARTIE V.1

Nomination du commissaire et durée du mandat

273.63

(1) Le gouverneur en Conseil peut nommer, à titre inamovible pour une période maximale de cinq ans, un juge surnuméraire ou un juge à la retraite d'une juridiction supérieure qu'il charge de remplir les fonctions de commissaire du Centre de la sécurité des télécommunications.

Mandat

(2) Le commissaire a pour mandat :

a) de procéder à des examens concernant les activités du Centre pour en contrôler la légalité;

b) de faire les enquêtes qu'il estime nécessaires à la suite de plaintes qui lui sont présentées;

c) d'informer le ministre et le procureur général du Canada de tous les cas où, à son avis, le Centre pourrait ne pas avoir agi en conformité avec la loi.

Rapport annuel

(3) Le commissaire adresse au ministre, dans les quatre-vingt-dix jours suivant la fin de chaque exercice, un rapport sur l'exercice de ses activités. Le ministre dépose le rapport devant chacune des chambres du Parlement dans les quinze premiers jours de séance de celle-ci suivant sa réception.

Loi sur les enquêtes

(4) Dans l'exercice de son mandat, le commissaire a tous les pouvoirs conférés à un commissaire en vertu de la partie II de la ***Loi sur les enquêtes***.

Assistance

(5) Le commissaire peut retenir les services de conseillers juridiques ou techniques ou d'autres collaborateurs dont la compétence lui est utile dans l'exercice de ses fonctions; il peut fixer, avec l'approbation du Conseil du Trésor, leur rémunération et leurs frais.

Fonctions du commissaire

(6) Le commissaire exerce les attributions que lui confèrent la présente partie et toute autre loi fédérale; il peut en outre se livrer à toute activité connexe autorisée par le gouverneur en conseil.

[...]

Révision des autorisations

273.65

(8) Le commissaire du Centre de la sécurité des télécommunications est tenu de faire enquête sur les activités qui ont été exercées sous le régime d'une autorisation donnée en vertu du présent article pour en contrôler la conformité; il rend compte de ses enquêtes annuellement au ministre.

LOI SUR LA PROTECTION DE L'INFORMATION

Défense d'intérêt public

15.

(1) Nul ne peut être déclaré coupable d'une infraction prévue aux articles 13 ou 14 s'il établit qu'il a agi dans l'intérêt public.

[...]

Informer les autorités

(5) Le juge ou le tribunal ne peut décider de la prépondérance des motifs d'intérêt public en faveur de la révélation que si la personne s'est conformée aux exigences suivantes : [...]

a) la personne, avant la communication ou la confirmation, a informé de la question [...] l'administrateur général ou [...] le sous-procureur général du Canada;

b) dans le cas où elle n'a pas reçu de réponse de l'administrateur général ou du sous-procureur général du Canada dans un délai raisonnable, elle a informé de la question, avec tous les renseignements à l'appui en sa possession, [...]

(ii) soit le commissaire du Centre de la sécurité des télécommunications si la question porte sur une infraction qui a été, est en train ou est sur le point d'être commise par un membre du Centre de la sécurité des télécommunications dans l'exercice effectif ou censé tel de ses fonctions pour le compte de celui-ci, et n'en a pas reçu de réponse dans un délai raisonnable.